ELSEVIER

Discrete Applied Mathematics 125 (2003) 289–318

DISCRETE APPLIED MATHEMATICS

Opacity of a finite automaton, method of calculation and the Ising chain

Jia-Yan Yao

Department of Mathematics, Nonlinear Science Center, Wuhan University, Wuhan 430072, People's Republic of China

Received 14 September 1999; received in revised form 9 February 2001; accepted 1 October 2001

Abstract

When a communication system transmits information, inevitably it will produce some noises which disturb the transmitted information. These noises may be caused by some physical or statistical reasons. The study of these exterior factors is very important and we can find in the literature many excellent books and articles about them. However, the most important causes are not exterior but interior ones which come from the internal structure of our communication system. In 1991, Michel Mendès France introduced the notion of opacity of a finite automaton, which is a good intuitive mathematical model for a communication system, and applied it to study the inhomogeneous Ising chain. Since then, opacity becomes an important tool in the study of noises produced during information transmission. In this work, we shall continue our study in opacity theory. More precisely, we shall give a general method to compute the opacity of any given finite automaton. As an application, we shall calculate the opacities of the Ising automata.

MSC: primary 68Q45; 18B20; secondary 68P30

Keywords: Opacity; Finite automaton; Ising chain

1. Introduction

When a communication system transmits information, it will inevitably produce some noises which disturb the transmitted information. These noises may be caused by some physical or statistical reasons. The study of these exterior factors is very important and we can find in the literature many excellent books and articles about them (see e.g. [6] and its references). However, the most important causes are not exterior but interior

E-mail address: yaojiaya@public.wh.hb.cn (J.-Y. Yao).

0166-218X/02/$ - see front matter
PII: S0166-218X(01)00363-8

ones which come from the internal structure of the system. In 1991, M. Mendès France introduced the notion of opacity of a finite automaton, which is a good mathematical model for a communication system, and applied it to study the inhomogeneous Ising chain. Since then, opacity becomes an important tool in the study of noises produced during transmission. In this work we shall continue our study launched in [8]. More precisely, we shall give a general method to calculate the opacity of any given finite automaton. As an application, we shall calculate the opacities of the Ising automata.

Vaguely speaking, a finite automaton $\mathscr{A}$ defined by a quadruplet (S, i, Σ, t) is a machine which transforms any sequence $\varepsilon = (\varepsilon(m))_{m \geqslant 0}$ over the alphabet $\Sigma \subseteq \mathbb{C}$ into another sequence $\mathscr{A}\varepsilon$ over the alphabet S. The opacity of $\mathscr{A}$ measures the distortion between the input sequence ε and the output sequence $\mathscr{A}\varepsilon$.

More precisely, $\forall q \in \mathbb{R}$ $(q \geqslant 1)$, the opacity $\Omega_q(\mathscr{A})$ of a finite automaton $\mathscr{A}$ is

$$\Omega_q(\mathscr{A}) = \sup_{\varepsilon} \inf_{\varphi} \limsup_{k \to \infty} \left(\frac{1}{k} \sum_{m=0}^{k-1} |\varphi(\mathscr{A}\varepsilon)(m) - \varepsilon(m)|^q \right)^{1/q}, \tag{1}$$

where $\varepsilon \in \Sigma^{\mathbb{N}}$, $\varphi \in \mathbb{C}^S$ and $\forall m \in \mathbb{N}$, we define $\varphi(\mathscr{A}\varepsilon)(m) := \varphi((\mathscr{A}\varepsilon)(m))$.

This quantity was originally defined and discussed by Mendès France in the case $q = 2$ and $S = \{-1, +1\}$ (see [5]). We can give different interpretations to this notion. Different interpretations lead to different applications in different research domains. For example, just as above, we can regard the finite automaton $\mathscr{A}$ as a transmitter of information, then $\Omega_q(\mathscr{A})$ is the inherent noise produced by the intrinsic default of $\mathscr{A}$. But if we treat $\mathscr{A}$ as a measuring instrument, then the quantity $\Omega_q(\mathscr{A})$ gives the precision of our instrument.

The aim of our study is double: on the one hand, we want to calculate $\Omega_q(\mathscr{A})$ in knowing the structural properties of $\mathscr{A}$, and on the other hand, given the opacity value $\Omega_q(\mathscr{A})$, we hope to devise the structure of $\mathscr{A}$ (if impossible for any value, it should be possible at least for some special values). The first one is relatively easy. Below we shall give an explicit method to calculate $\Omega_q(\mathscr{A})$ with $q = 2$ (see also [7]). The second one is more difficult. The difficulty consists in the fact that the geometry of the set Σ plays a decisive role in the study. Until now we only have some partial results about this problem. For example, we know how to characterize all the transparent automata, i.e., those automata whose opacities are minimal (in fact, the minimal value is zero) and we can also characterize all the opaque automata whose opacities are maximal (see [7,8,1]).

This work can be regarded as a natural continuation of [8] where we have already presented some general properties of the opacity of a finite automaton. But for the convenience of our potential readers, we have made efforts so that this article can be read independently of [8].

2. Notion of finite automaton

Let E be an alphabet, i.e., a finite nonempty set. The number of elements in E is denoted by $Card(E)$. Let $m \in \mathbb{N}$ $(m \geqslant 1)$. Each element of E^m is called a word (or

sequence) of length m over E. By convention we put $E^0 = \{\emptyset\}$, where $\emptyset$ is the empty word of length 0. And we define

$$E^* := \bigcup_{m \geqslant 0} E^m \quad \text{and} \quad \bar{E} := E^* \cup E^{\mathbb{N}},$$

where $\mathbb{N} = \{0, 1, \ldots\}$ is the set of natural numbers, i.e., nonnegative integers. For any finite or infinite sequence $u = (u(m))_{m \geqslant 0} \in \bar{E}$, the length of u is denoted by $|u|$. Evidently $|u|$ is an element in $\mathbb{N} \cup \{\infty\}$.

Now we give below a definition of finite automaton (see for example [2]):

A finite automaton $\mathscr{A} = (S, i, \Sigma, t)$ (called Σ-automaton) consists of

- an alphabet S of states; one of the states, say i, is distinguished and called initial state.
- a mapping $t : S \times \Sigma \to S$, called transition function where Σ is an alphabet containing at least two elements.

Conventionally, we put $t(A, \emptyset) = A$ for any $A \in S$. Then we extend the mapping t over $S \times \Sigma^*$ (denoted again by t) such that

$$\forall A \in S \text{ and } \forall \sigma, \eta \in \Sigma^*, \text{ we have } t(A, \sigma\eta) := t(t(A, \sigma), \eta).$$

The Σ-automaton $\mathscr{A}$ induces also a mapping (denoted still by $\mathscr{A}$) from $\bar{\Sigma}$ to $\bar{S}$ such that for any $\varepsilon \in \bar{\Sigma}$ and $m \in \mathbb{N}$ $(0 \leqslant m < |\varepsilon|)$, we have $(\mathscr{A}\varepsilon)(m) := t(i, \varepsilon(0) \cdots \varepsilon(m))$. This mapping $\mathscr{A}$ will be the kernel of our later study.

Remark that we have not mentioned here the notion of terminal state, that the preceding definition corresponds to the classical notion of complete (deterministic) automaton where all states are final (cf. [2]), and that we do not want to recognize a language, but only consider the finite automaton as a machine which transforms a sequence into another one.

It is useful to give a pictorial representation of $\mathscr{A}$. States are represented by points or nodes or vertices. For any $A \in S$ and any $\sigma \in \Sigma$, we link A to $t(A, \sigma)$ by a (directed) arrow, labelled σ. This arrow (called also edge) is said of type σ and denoted by $(A, \sigma, t(A, \sigma))$ (i.e., treated as an element in $S \times \Sigma \times S$) where A is the starting-point, σ is the label or type of the arrow and $t(A, \sigma)$ is the endpoint. In the following, we shall constantly identify $\mathscr{A}$ with its graph. Then S becomes the set of vertices and Σ becomes the set of labels or types of arrows.

Let $\mathscr{A} = (S, i, \Sigma, t)$ be a finite automaton. We call $\mathscr{A}$ a connected automaton if on the graph of $\mathscr{A}$, any vertex of $\mathscr{A}$ can be reached from the initial state i, i.e., the graph of $\mathscr{A}$ is connected, or more precisely, for any $A \in S$, we can find $\sigma \in \Sigma^*$ such that $A = t(i, \sigma)$. Later we shall only study connected Σ-automata with $\Sigma \subseteq \mathbb{C}$.

3. Opacity of a finite automaton

Fix $q \in \mathbb{R}$ $(q \geqslant 1)$. For every bounded complex sequence $u = (u(m))_{m \geqslant 0}$, the seminorm $||u||_q$ of u is defined as

$$||u||_q := \limsup_{k \to \infty} \left(\frac{1}{k} \sum_{m=0}^{k-1} |u(m)|^q \right)^{1/q}.$$

And the opacity $\Omega_q(\mathscr{A})$, of a finite automaton $\mathscr{A} = (S, i, \Sigma, t)$, is

$$\Omega_q(\mathscr{A}) = \sup_{\varepsilon} \inf_{\varphi} ||\varphi(\mathscr{A}\varepsilon) - \varepsilon||_q,$$

where $\varepsilon \in \Sigma^{\mathbb{N}}$, $\varphi \in \mathbb{C}^S$ and $\varphi(\mathscr{A}\varepsilon) := (\varphi((\mathscr{A}\varepsilon)(m)))_{m \geqslant 0}$.

The motivation of the preceding definition is quite evident and instructive. In fact, it is related to the following general question:

given a machine $\mathscr{A}$, how can we measure its inherent noise?

For this, we should do experiments on $\mathscr{A}$. An experiment consists in feeding $\mathscr{A}$ with an input sequence $\varepsilon = (\varepsilon(m))_{m \geqslant 0}$. The result is an output sequence $\mathscr{A}\varepsilon$ which acts on some measuring instrument φ and allows us to read $\varphi(\mathscr{A}\varepsilon)$ a sequence of numbers. Compute the distance between $\varphi(\mathscr{A}\varepsilon)$ and ε, we obtain $d(\varphi(\mathscr{A}\varepsilon), \varepsilon)$ which is the distortion of the experiment ε. Refine our measuring instrument φ to minimize errors caused by φ. The inherent noise $\Omega^d(\mathscr{A})$ of $\mathscr{A}$ is defined by

$$\Omega^d(\mathscr{A}) = \sup_{\varepsilon} \inf_{\varphi} d(\varphi(\mathscr{A}\varepsilon), \varepsilon).$$

It is clear that $\Omega^d(\mathscr{A})$ is the greatest distortion of all experiments and our opacity function Ω_q is a special Ω^d-function (see [8] for some general discussions of Ω^d).

But we can also exchange the preceding procedure, i.e., first fix the measuring instrument φ and compute the greatest distortion $\sup_{\varepsilon} d(\varphi(\mathscr{A}\varepsilon), \varepsilon)$, then refine our measuring instruments to delete the noises produced by them. Finally we obtain

$$\Phi^d(\mathscr{A}) = \inf_{\varphi} \sup_{\varepsilon} d(\varphi(\mathscr{A}\varepsilon), \varepsilon)$$

which is another type of opacity. Clearly $\Phi^d(\mathscr{A}) \geqslant \Omega^d(\mathscr{A})$. If the strict inequality holds (this is possible as we can see in [8]), we meet a bad situation as it contradicts our usual concept. Fortunately in the case of Ω_q, with the help of the Minimax Theorem of J. von Neumann, we already showed in [8] (see also Theorem 5 below) that for any finite automaton $\mathscr{A}$, holds the equality $\Omega_q(\mathscr{A}) = \inf_{\varphi} \sup_{\varepsilon} ||\varphi(\mathscr{A}\varepsilon) - \varepsilon||_q$.

Given a finite automaton, it is difficult to calculate $\Omega_q(\mathscr{A})$ directly from its definition. To avoid this difficulty, Mendès France introduced (cf. [5])

$$\omega_q(\mathscr{A}) = \sup_{\varepsilon\, u.p} \inf_{\varphi} ||\varphi(\mathscr{A}\varepsilon) - \varepsilon||_q,$$

where φ is a complex valued function defined on S and ε $u.p$ means that ε is ultimately periodic. In fact, he only studied $\omega_2(\mathscr{A})$ and conjectured $\omega_2(\mathscr{A}) = \Omega_2(\mathscr{A})$ which is a special case of the general equality $\omega_q(\mathscr{A}) = \Omega_q(\mathscr{A})$ already proved in [8]. Later we shall give another proof of the equality $\omega_2(\mathscr{A}) = \Omega_2(\mathscr{A})$ in Theorem 3.

Below we show a sharp bound for Ω_q to finish this section.

Denote by $\mathscr{I}_\Sigma$ a Σ-automaton having only one state (there are infinitely many Σ-automata of this kind. However their difference consists only in their notations of the state but not in the structure. So we can regard them identical). Trivially

$$\Omega_q(\mathscr{I}_\Sigma) = \sup_{\varepsilon} \inf_{x \in \mathbb{C}} ||\bar{x} - \varepsilon||_q, \tag{2}$$

where $\varepsilon \in \Sigma^{\mathbb{N}}$ and $\bar{x}$ indicates the constant sequence of common value x.

Then for every Σ-automaton $\mathscr{A} = (S, i, \Sigma, t)$, we have

$$\Omega_q(\mathscr{A}) = \sup_{\varepsilon} \inf_{\varphi} ||\varphi(\mathscr{A}\varepsilon) - \varepsilon||_q \leqslant \sup_{\varepsilon} \inf_{x \in \mathbb{C}} ||\bar{x} - \varepsilon||_q = \Omega_q(\mathscr{I}_\Sigma)$$

by putting $\varphi \equiv x$ in the first inf. Then we obtain $0 \leqslant \Omega_q(\mathscr{A}) \leqslant \Omega_q(\mathscr{I}_\Sigma)$ which is a sharp bound for the opacity function Ω_q.

Remark that the quantity $\Omega_q(\mathscr{I}_\Sigma)$ depends only on Σ and may be large if we choose Σ correctly. In fact, we have the equality (see [1] or Corollary 3 below)

$$\Omega_q(\mathscr{I}_\Sigma) = \min_{x \in \mathbb{C}} \max_{\sigma \in \Sigma} |x - \sigma|.$$

Hence the precise value of $\Omega_q(\mathscr{A})$ cannot truly reflect the structural complexity of $\mathscr{A}$. It is better for us to consider the opacity ratio $\rho_q(\mathscr{A}) := \Omega_q(\mathscr{A})/\Omega_q(\mathscr{I}_\Sigma)$ which removes a little the influence of the size of Σ. We say a finite automaton $\mathscr{A}$ transparent (resp. opaque) if $\rho_q(\mathscr{A}) = 0$ (resp. $\rho_q(\mathscr{A}) = 1$). The reader can consult [7,8,1] for the characterization of transparent (resp. opaque) automata.

From now on, we shall concentrate our study on the case $q=2$ and write $\Omega, \omega, ||\cdot||, \ldots$ instead of $\Omega_2, \omega_2, ||\cdot||_2, \ldots$.

4. Circuits on the graph of a finite automaton

We will study here the circuits on the graph of a finite automaton and show some of their basic properties.

Let $\mathscr{A} = (S, i, \Sigma, t)$ be a finite automaton. A finite or infinite (directed) path $\mathscr{P}$ on (the graph of) $\mathscr{A}$ is a finite or infinite sequence of successive directed arrows. The length of $\mathscr{P}$ (denoted by $\ell(\mathscr{P})$) is the number of directed arrows contained in $\mathscr{P}$. Since a directed arrow on $\mathscr{A}$ is regarded as an element of $S \times \Sigma \times S$, so any path $\mathscr{P}$ can be represented by a sequence over $S \times \Sigma \times S$ and we often identify $\mathscr{P}$ with this sequence. Intuitively we can identify every path $\mathscr{P}$ with the set of its arrows counted with multiplicity, i.e., when we move along $\mathscr{P}$, if we have met m times the same arrow, we count it as m different arrows. Obviously, every path $\mathscr{P}$ on $\mathscr{A}$ is determined uniquely by its starting-point and by $\varepsilon[\mathscr{P}] \in \bar{\Sigma}$ the sequence of labels (called the label of $\mathscr{P}$) appearing in $\mathscr{P}$. Conversely, any $\varepsilon = (\varepsilon(m))_{m \geqslant 0} \in \bar{\Sigma}$ generates a path $\mathscr{P}(\varepsilon) := (i, \varepsilon(0), (\mathscr{A}\varepsilon)(0))((\mathscr{A}\varepsilon)(0), \varepsilon(1), (\mathscr{A}\varepsilon)(1)) \cdots$ on $\mathscr{A}$. Clearly we have the relation $\varepsilon[\mathscr{P}(\varepsilon)] = \varepsilon$.

A circuit $\mathscr{C}$ on $\mathscr{A}$ is a cyclic directed path on the graph of $\mathscr{A}$. As above the circuit $\mathscr{C}$ can also be represented by a finite sequence over $S \times \Sigma \times S$ and we often identify $\mathscr{C}$ with this sequence. A circuit possesses a point of base or starting-point. To change the point of base is to change the circuit, which is deduced from the first one by a circular permutation (however in the concrete calculation of the opacity of a finite automaton, we need not make this distinction. See Sections 5 and 9). Denote by $\mathfrak{C}(\mathscr{A})$ the set of all circuits on $\mathscr{A}$. It is evident that $\mathfrak{C}(\mathscr{A})$ is nonempty and denumerable as $\mathscr{A}$ is connected and only possesses a finite number of states. We shall see that $\mathfrak{C}(\mathscr{A})$ has a very simple structure.

Let $\mathscr{C}'$ and $\mathscr{C}''$ be two circuits of $\mathscr{A}$ with A' and A'' as their points of base. If A'' is a vertex of $\mathscr{C}'$, by concatenation, we can define a new circuit of $\mathscr{A}$ (denoted by

$\mathscr{C}'\mathscr{C}''$) as follows. Write $\mathscr{C}' = L_1 \cdots L_k \cdots L_m$ with $L_j \in S \times \Sigma \times S$ $(1 \leqslant j \leqslant m)$ such that A' is the starting-vertex of L_1, A'' is the end-vertex of L_k and A'' does not appear in L_j for any integer j $(1 \leqslant j < k)$. Then we define $\mathscr{C}'\mathscr{C}'' := L_1 \cdots L_k \mathscr{C}'' L_{k+1} \cdots L_m$. We may give an intuitive explication of this definition. We begin with A' taken as the starting-point of $\mathscr{C}'\mathscr{C}''$ and run through $\mathscr{C}'$ until we meet A'' for the first time. Then we leave $\mathscr{C}'$ for $\mathscr{C}''$ and run through $\mathscr{C}''$ until we have visited all the vertices of $\mathscr{C}''$. Now we are at A'' again and we continue the rest of $\mathscr{C}'$.

Let $\mathscr{C}$ be a circuit of $\mathscr{A}$. We call $\mathscr{C}$ a simple circuit if any vertex of $\mathscr{C}$ possesses only one inward arrow and only one outward arrow. Since $\mathscr{A}$ only has a finite number of vertices, there only exists a finite number of simple circuits, say $\mathscr{C}_1, \mathscr{C}_2, \ldots, \mathscr{C}_n$. Consider the free $\mathbb{Z}$-module generated by all these simple circuits whose elements can be expressed by formal sums $\sum_{j=1}^{n} a_j \mathscr{C}_j$ with $a_j \in \mathbb{Z}$. A circuit $\mathscr{C}$ of $\mathscr{A}$ is said representable by (or pass through) a formal sum $\sum_{j=1}^{n} a_j \mathscr{C}_j$ with $a_j \in \mathbb{N}$ (for simplicity, we often write directly $\mathscr{C} = \sum_{j=1}^{n} a_j \mathscr{C}_j$) if there exists a decomposition of this formal sum by simple circuits of the form $\mathscr{C}_{i_1} + \mathscr{C}_{i_2} + \cdots + \mathscr{C}_{i_m}$ (the order being significative), where for each integer j $(1 \leqslant j \leqslant n)$, the simple circuit $\mathscr{C}_j$ appears exactly a_j times, so that by concatenation we have $\mathscr{C} = \mathscr{C}_{i_1}\mathscr{C}_{i_2} \cdots \mathscr{C}_{i_m}$. By induction on the length of the circuit in discussion, we can easily show that every circuit can be represented by a formal sum of simple circuits. However, the representation is not necessarily unique. In other words, given a circuit $\mathscr{C}$, we can find a point $a(\mathscr{C}) = (a_j(\mathscr{C}))_{1 \leqslant j \leqslant n}$ in $\mathbb{N}^n \setminus \{O\}$ such that $\mathscr{C}$ passes through the formal sum $\sum_{j=1}^{n} a_j(\mathscr{C})\mathscr{C}_j$ and in general, such a point $a(\mathscr{C})$ is not unique (cf. [7,8]). We shall see later that this nuisance does not trouble the pursuit of our study.

Let $\mathscr{P} = P_0 P_1 \cdots$ with $P_j \in S \times \Sigma \times S$ be an infinite path on the graph of $\mathscr{A}$. Let $\mathscr{C} = L_0 L_1 \cdots L_{m-1}$ $(L_j \in S \times \Sigma \times S)$ be a circuit on $\mathscr{A}$. We say that the path $\mathscr{P}$ ultimately winds up on $\mathscr{C}$ if $\exists\, d \in \mathbb{N}$ such that $\forall\, j, k \in \mathbb{N}$, we have $P_{j+d} = L_k$ if and only if $j \equiv k \pmod{m}$. Clearly this definition is just a mathematical reformulation of our geometrical intuition.

Let $\mathscr{C}$ be a circuit on $\mathscr{A}$ with $A \in S$ as its point of base. Since $\mathscr{A}$ is connected, we can find a word $\sigma \in \Sigma^*$ such that $A = t(i, \sigma)$. Let δ be the label of $\mathscr{C}$. Then $\varepsilon_{\mathscr{C}} := \sigma\delta^{\infty} := \sigma\delta\delta \cdots$ is an ultimately periodic sequence such that the infinite path $\mathscr{P}(\varepsilon_{\mathscr{C}})$ generated by $\varepsilon_{\mathscr{C}}$ ultimately winds up on $\mathscr{C}$. Conversely, for any ultimately periodic sequence ε, we can easily prove that there exists a circuit $\mathscr{C}_{\varepsilon}$ on $\mathscr{A}$ such that the path $\mathscr{P}(\varepsilon)$ generated by ε ultimately winds up on $\mathscr{C}_{\varepsilon}$ (cf. [7,8]). Later we shall use implicitly this remark in many different occasions.

5. Algorithm to compute the opacity of a finite automaton

Below we shall present an effective algorithm to compute the opacity of any given automaton.

We begin with some preliminary definitions and notations.

Let $\mathscr{A} = (S, i, \Sigma, t)$ be a finite automaton and $\mathscr{C}_1, \ldots, \mathscr{C}_n$ be its simple circuits. Let $A \in S$ and $\sigma \in \Sigma$. For any $j \in \mathbb{N}$ $(1 \leqslant j \leqslant n)$, define $\delta_{\sigma}^{j}(A) := 1$ if A is a vertex of $\mathscr{C}_j$ and on $\mathscr{C}_j$, the inward arrow into A is of type σ. Otherwise put $\delta_{\sigma}^{j}(A) := 0$.

Let $a=(a_1,\ldots,a_n)\in\mathbb{R}^n_+\setminus\{O\}$, i.e., $a_j\geqslant 0$ $(1\leqslant j\leqslant n)$ and a is different from the origin of coordinates. For any $A\in S$ and $\sigma\in\Sigma$, define

$$\lambda_{A,\sigma}(a)=\sum_{j=1}^{n}a_j\delta^j_\sigma(A),\quad \lambda_A(a)=\sum_{\eta\in\Sigma}\lambda_{A,\eta}(a)\quad\text{and}\quad \lambda(a)=\sum_{B\in S}\lambda_B(a). \tag{3}$$

Obviously for any $j\in\mathbb{N}$ $(1\leqslant j\leqslant n)$ and for any $A\in S$, $\sum_{\sigma\in\Sigma}\delta^j_\sigma(A)$ is the number of arrows on $\mathscr{C}_j$ which enters A. This number equals 0 or 1 and it equals 1 if and only if A is a vertex in $\mathscr{C}_j$. Recall that $\ell(\mathscr{C}_j)$ is the length of $\mathscr{C}_j$, i.e., the number of arrows contained in $\mathscr{C}_j$. And it is also the number of vertices in $\mathscr{C}_j$. Thus we obtain

$$\ell(\mathscr{C}_j)=\sum_{A\in S}\sum_{\sigma\in\Sigma}\delta^j_\sigma(A).$$

So for any $a=(a_1,\ldots,a_n)\in\mathbb{R}^n_+\setminus\{O\}$, we have

$$\lambda(a)=\sum_{A\in S}\lambda_A(a)=\sum_{A\in S}\sum_{\sigma\in\Sigma}\sum_{j=1}^{n}a_j\delta^j_\sigma(A)=\sum_{j=1}^{n}a_j\ell(\mathscr{C}_j). \tag{4}$$

Let $\mathscr{C}$ be a circuit on $\mathscr{A}$. Then we can find $a(\mathscr{C})=(a_j(\mathscr{C}))_{1\leqslant j\leqslant n}\in\mathbb{R}^n_+\setminus\{O\}$ such that $\mathscr{C}=\sum_{j=1}^{n}a_j(\mathscr{C})\mathscr{C}_j$. It is clear that $\lambda(a(\mathscr{C}))$ is the length of $\mathscr{C}$ and $\lambda_{A,\sigma}(a(\mathscr{C}))$ (with $\sigma\in\Sigma$ and $A\in S$) is the number of arrows of type σ on $\mathscr{C}$ which enter A. These numbers only depend on the circuit $\mathscr{C}$ but neither on the special choice of the point $a(\mathscr{C})$ nor on the point of base of $\mathscr{C}$.

Let A be a vertex of $\mathscr{A}$. For any point $a=(a_1,\ldots,a_n)\in\mathbb{R}^n_+\setminus\{O\}$, define

$$G_A(a):=\inf_{x\in\mathbb{C}}\sum_{\sigma\in\Sigma}\lambda_{A,\sigma}(a)|x-\sigma|^2.$$

The infimum is attained at the complex number $\varphi_a(A)$ defined by

$$\varphi_a(A):=\frac{1}{\lambda_A(a)}\sum_{\sigma\in\Sigma}\lambda_{A,\sigma}(a)\sigma$$

if $\lambda_A(a)>0$ and $\varphi_a(A):=0$ otherwise (in fact in this case $\varphi_a(A)$ can be arbitrary). In this way, we define on S a complex valued function φ_a which will be used soon.

If $\lambda_A(a)=0$, then $G_A(a)=0$. Otherwise $\lambda_A(a)>0$ and we have

$$G_A(a)=\frac{1}{2\lambda_A(a)}\sum_{\sigma,\eta\in\Sigma}\lambda_{A,\sigma}(a)\lambda_{A,\eta}(a)|\sigma-\eta|^2\leqslant\frac{1}{2}\lambda_A(a)\max_{\sigma,\eta\in\Sigma}|\sigma-\eta|^2.$$

Thus G_A is rational and continuous on $\mathbb{R}^n_+\setminus\{O\}$. But in general, this function is not differentiable. It only possesses weak partial derivatives defined as follows.

Let f be a function defined on $\mathbb{R}^n_+\setminus\{O\}$. We say that f possesses a weak partial derivative at $a^0=(a^0_1,\ldots,a^0_n)$ with respect to its jth variable a_j $(1\leqslant j\leqslant n)$, if the following limit exists (and it will be denoted by $\partial f/\partial a_j(a^0)$),

$$\lim_{x\to 0}\frac{1}{x}(f(a^0_1,\ldots,a^0_j+x,\ldots,a^0_n)-f(a^0_1,\ldots,a^0_j,\ldots,a^0_n)),$$

where x varies in $\mathbb{R}$ so that $(a^0_1,\ldots,a^0_j+x,\ldots,a^0_n)\in\mathbb{R}^n_+\setminus\{O\}$.

Let $A \in S$ be a vertex of $\mathscr{A}$. For any $a^0 \in \mathbb{R}_+^n \setminus \{O\}$ and any $j \in \mathbb{N}$ $(1 \leqslant j \leqslant n)$, we shall show below that at the point a^0, the function G_A possesses a weak partial derivative with respect to its jth variable a_j.

If A is not a vertex of $\mathscr{C}_j$, then G_A is independent of a_j. Consequently, G_A is differentiable with respect to its jth variable and $\partial G_A/\partial a_j(a^0) = 0$. So we need only consider the case that A is a vertex of $\mathscr{C}_j$. There are only two possibilities.

Case 1: $\lambda_A(a^0) > 0$. Then a^0 is a regular point of G_A. Thus at the point a^0, the rational function G_A is differentiable with respect to its jth variable, a fortiori, it possesses a weak partial derivative.

Case 2: $\lambda_A(a^0) = 0$. Then $G_A(a^0) = 0$. Let e_j be the jth element of the canonical basis of the $\mathbb{R}$-vector space $\mathbb{R}^n$, i.e., $e_j = (0, \ldots, 1, \ldots, 0)$ where only the jth coordinate of e_j is not zero and it equals 1. Let $r > 0$ be a real number. For any $\sigma \in \Sigma$, we have $\lambda_{A,\sigma}(a^0 + re_j) = r\delta_\sigma^j(A)$. Hence

$$G_A(a^0 + re_j) = 0 \quad \text{and} \quad \lambda_A(a^0 + re_j) = r\sum_{\sigma\in\Sigma} \delta_\sigma^j(A) = r$$

for A is a vertex of $\mathscr{C}_j$. So $\partial G_A/\partial a_j(a^0) = 0$ in the weak sense.

Finally, for any point $a = (a_1, \ldots, a_n) \in \mathbb{R}_+^n \setminus \{O\}$ and any $\varphi \in \mathbb{C}^S$, define

$$G(a, \varphi) := \sum_{A\in S}\sum_{\sigma\in\Sigma} \lambda_{A,\sigma}(a)|\varphi(A) - \sigma|^2 \quad \text{and} \quad v(a) := \inf_{\phi\in\mathbb{C}^S} G(a, \phi). \tag{5}$$

Then we obtain

$$\begin{aligned} v(a) &= \inf_{\phi\in\mathbb{C}^S} \sum_{A\in S}\sum_{\sigma\in\Sigma} \lambda_{A,\sigma}(a)|\phi(A) - \sigma|^2 \\ &= \sum_{A\in S} \inf_{\phi\in\mathbb{C}^S} \sum_{\sigma\in\Sigma} \lambda_{A,\sigma}(a)|\phi(A) - \sigma|^2 \\ &= \sum_{A\in S} G_A(a) \\ &= \sum_{A\in S}\sum_{\sigma\in\Sigma} \lambda_{A,\sigma}(a)|\varphi_a(A) - \sigma|^2 \\ &= G(a, \varphi_a) \end{aligned} \tag{6}$$

for all the values $\phi(A)$ $(A \in S)$ of $\phi \in \mathbb{C}^S$ can be chosen independently. Hence the function v also possesses weak partial derivatives on $\mathbb{R}_+^n \setminus \{O\}$.

With these notations and definitions, we have the following theorem which generalizes, completes and corrects a result of [5]. Remark also that our notations do not coincide exactly with those of Mendès France.

Theorem 1. *Let $\mathscr{A} = (S, i, \Sigma, t)$ be a finite automaton. Then we have*

$$\omega(\mathscr{A}) = \sup_{a\in\mathbb{R}_+^n\setminus\{O\}} \sqrt{\frac{v(a)}{\lambda(a)}}. \tag{7}$$

Proof. Let ε be an ultimately periodic sequence of labels. Then there exists a circuit $\mathscr{C}_\varepsilon$ on $\mathscr{A}$ such that the infinite path $\mathscr{P}(\varepsilon)$ generated by ε ultimately winds up on $\mathscr{C}_\varepsilon$. For the circuit $\mathscr{C}_\varepsilon$, we can find a point $a(\mathscr{C}_\varepsilon) = (a_j(\mathscr{C}_\varepsilon))_{1\leqslant j\leqslant n} \in \mathbb{N}^n \setminus \{O\}$ such that $\mathscr{C}_\varepsilon = \sum_{j=1}^n a_j(\mathscr{C}_\varepsilon)\mathscr{C}_j$. Then for any $\varphi \in \mathbb{C}^S$, we have trivially

$$||\varphi(\mathscr{A}\varepsilon) - \varepsilon|| = \sqrt{\frac{G(a(\mathscr{C}_\varepsilon), \varphi)}{\lambda(a(\mathscr{C}_\varepsilon))}}. \tag{8}$$

Conversely let $\mathscr{C}$ be a circuit. Then there exists an ultimately periodic sequence of labels $\varepsilon_{\mathscr{C}}$ such that the infinite path $\mathscr{P}(\varepsilon_{\mathscr{C}})$ generated by $\varepsilon_{\mathscr{C}}$ ultimately winds up on $\mathscr{C}$. Let $a(\mathscr{C}) = (a_j(\mathscr{C}))_{1\leqslant j\leqslant n}$ be a point $\mathbb{N}^n \setminus \{O\}$ such that $\mathscr{C} = \sum_{j=1}^n a_j(\mathscr{C})\mathscr{C}_j$. Then for any $\varphi \in \mathbb{C}^S$, we also have

$$||\varphi(\mathscr{A}\varepsilon_{\mathscr{C}}) - \varepsilon_{\mathscr{C}}|| = \sqrt{\frac{G(a(\mathscr{C}), \varphi)}{\lambda(a(\mathscr{C}))}}. \tag{9}$$

As a result, we obtain the following equality

$$\omega(\mathscr{A}) = \sup_{\mathscr{C}\in\mathfrak{C}(\mathscr{A})} \inf_{\varphi\in\mathbb{C}^S} \sqrt{\frac{G(a(\mathscr{C}), \varphi)}{\lambda(a(\mathscr{C}))}} = \sup_{\mathscr{C}\in\mathfrak{C}(\mathscr{A})} \sqrt{\frac{v(a(\mathscr{C}))}{\lambda(a(\mathscr{C}))}}, \tag{10}$$

where $\mathfrak{C}(\mathscr{A})$ is the set of all circuits of $\mathscr{A}$.

Take $a = (a_j)_{1\leqslant j\leqslant n}$ in $\mathbb{N}^n \setminus \{O\}$ and consider the formal sum $\mathscr{P} := \sum_{j=1}^n a_j\mathscr{C}_j$. Remark that two circuits $\mathscr{C}$ and $\mathscr{C}'$, represented by formal sums $\mathscr{F}$ and $\mathscr{F}'$, when they have a common vertex A, determine a circuit $\mathscr{C}''$ (with A as the point of base) which passes through the formal sum $\mathscr{F} + \mathscr{F}'$. Thus we can decompose the formal sum $\mathscr{P}$ into $\mathscr{P} := \sum_{j=1}^m \mathscr{P}'_j$, where each formal sum $\mathscr{P}'_j$ represents a circuit $\mathscr{C}'_j$ and there is not common vertex between any two different $\mathscr{C}'_j$ (disjointed circuits). For each integer j $(1 \leqslant j \leqslant m)$, we can find a point $a(\mathscr{C}'_j) = (a_k(\mathscr{C}'_j))_{1\leqslant k\leqslant n}$ in $\mathbb{N}^n \setminus \{O\}$ such that $\mathscr{C}'_j = \sum_{k=1}^n a_k(\mathscr{C}'_j)\mathscr{C}_k$. Clearly for any $\varphi \in \mathbb{C}^S$, we have

$$G(a, \varphi) = \sum_{j=1}^m G(a(\mathscr{C}'_j), \varphi) \quad \text{and} \quad \lambda(a) = \sum_{j=1}^m \lambda(a(\mathscr{C}'_j)). \tag{11}$$

Since all these circuits $\mathscr{C}'_j$ are disjointed, then we obtain

$$v(a) = \inf_{\varphi\in\mathbb{C}^S} G(a, \varphi) = \sum_{j=1}^m \inf_{\varphi\in\mathbb{C}^S} G(a(\mathscr{C}'_j), \varphi) = \sum_{j=1}^m v(a(\mathscr{C}'_j)). \tag{12}$$

But for all positive numbers x, y, w and v, holds the trivial inequality

$$\frac{x+w}{y+v} \leqslant \max\left(\frac{x}{y}, \frac{w}{v}\right). \tag{13}$$

Then from Relations (11)–(13) and (10), we deduce

$$\sqrt{\frac{v(a)}{\lambda(a)}} = \sqrt{\frac{\sum_{j=1}^m v(a(\mathscr{C}'_j))}{\sum_{j=1}^m \lambda(a(\mathscr{C}'_j))}} \leqslant \max_{1\leqslant j\leqslant m} \sqrt{\frac{v(a(\mathscr{C}'_j))}{\lambda(a(\mathscr{C}'_j))}} \leqslant \omega(\mathscr{A}).$$

But trivially we also have

$$\omega(\mathscr{A}) = \sup_{\mathscr{C}\in\mathfrak{C}(\mathscr{A})} \sqrt{\frac{v(a(\mathscr{C}))}{\lambda(a(\mathscr{C}))}} \leqslant \sup_{a\in\mathbb{N}^n\setminus\{O\}} \sqrt{\frac{v(a)}{\lambda(a)}}.$$

In conclusion we have just shown the equality

$$\omega(\mathscr{A}) = \sup_{a\in\mathbb{N}^n\setminus\{O\}} \sqrt{\frac{v(a)}{\lambda(a)}}.$$

However, every positive real number can be approximated by positive rationals, and the function v/λ is rational and homogeneous of degree 0, so we have

$$\omega(\mathscr{A}) = \sup_{a\in\mathbb{R}_+^n\setminus\{O\}} \sqrt{\frac{v(a)}{\lambda(a)}}.$$

This ends the proof of our theorem. □

Corollary 1. *Let $\mathscr{A}=(S,i,\Sigma,t)$ be a finite automaton and $\mathscr{C}_1,\mathscr{C}_2,\ldots,\mathscr{C}_n$ be its simple circuits. Then we can find $a\in\mathbb{R}_+^n\setminus\{O\}$ such that $\omega(\mathscr{A})=\sqrt{v(a)/\lambda(a)}$.*

Proof. Put $E=\{a\mid a\in\mathbb{R}_+^n\setminus\{O\} \text{ and } \lambda(a)=1\}$. Clearly E is a compact subset of $\mathbb{R}_+^n\setminus\{O\}$. Since the function v/λ is rational and homogeneous of degree 0, then

$$\omega(\mathscr{A}) = \sup_{a\in\mathbb{R}_+^n\setminus\{O\}} \sqrt{\frac{v(a)}{\lambda(a)}} = \sup_{a\in E} \sqrt{v(a)}.$$

Thus we can find a point $a\in E\subseteq\mathbb{R}_+^n\setminus\{O\}$ such that $\omega(\mathscr{A})=\sqrt{v(a)/\lambda(a)}$ for the function v is continuous on the compact set E. □

Therefore, to compute the opacity $\omega(\mathscr{A})$, we need only find the maximum of v/λ. For this, we introduce an auxiliary function H^ω ($\omega\in\mathbb{R}_+$) defined on $\mathbb{R}_+^n\setminus\{O\}$ such that for any point $a\in\mathbb{R}_+^n\setminus\{O\}$, we have

$$H^\omega(a)=\lambda(a)\omega^2-v(a).$$

Obviously for any $\omega\in\mathbb{R}_+$, just like the functions v and λ, the function H^ω also possesses weak partial derivatives over $\mathbb{R}_+^n\setminus\{O\}$.

Now we give an algorithm to compute the opacity of a given automaton (cf. [7]).

Theorem 2. *Let $\mathscr{A}=(S,i,\Sigma,t)$ be a finite automaton and $\mathscr{C}_1,\mathscr{C}_2,\ldots,\mathscr{C}_n$ be its simple circuits. Let ω be a positive number. Then $\omega=\omega(\mathscr{A})$ if and only if there exists a point $a^\omega=(a_1^\omega,\ldots,a_n^\omega)\in\mathbb{R}_+^n\setminus\{O\}$ such that for any $j\in\mathbb{N}$ $(1\leqslant j\leqslant n)$, we have $\partial H^\omega/\partial a_j(a^\omega)\geqslant 0$ and if $a_j^\omega>0$, then $\partial H^\omega/\partial a_j(a^\omega)=0$.*

Proof. Put $\omega=\omega(\mathscr{A})$. Then ω is a positive number. By virtue of Corollary 1, we can find a point $a^\omega=(a_1^\omega,\ldots,a_n^\omega)\in\mathbb{R}_+^n\setminus\{O\}$ such that $\omega=\sqrt{v(a^\omega)/\lambda(a^\omega)}$. Therefore $H^\omega(a^\omega)=\lambda(a^\omega)\omega^2-v(a^\omega)=0$. Moreover by Theorem 1, for any point $a\in\mathbb{R}_+^n\setminus\{O\}$, we have $\omega\geqslant\sqrt{v(a)/\lambda(a)}$. Thus $H^\omega(a)=\lambda(a)\omega^2-v(a)\geqslant 0$ and a^ω is a global minimal

point of H^ω. Then from the definition of weak partial derivatives, we know that the point a^ω should verify the conditions of our theorem.

Conversely, let ω be a positive number such that there exists a point $a^\omega \in \mathbb{R}_+^n \setminus \{O\}$ satisfying the hypothesis of our theorem. We shall show that for any $a \in \mathbb{R}_+^n \setminus \{O\}$, we have $H^\omega(a) \geqslant H^\omega(a^\omega) = 0$ which implies immediately

$$\omega = \sqrt{v(a^\omega)/\lambda(a^\omega)} = \sup_{a \in \mathbb{R}_+^n \setminus \{O\}} \sqrt{\frac{v(a)}{\lambda(a)}} = \omega(\mathscr{A}).$$

Recall that by Formula (6), we have, for any point $a \in \mathbb{R}_+^n \setminus \{O\}$,

$$v(a) := \inf_{\phi \in \mathbb{C}^S} G(a, \phi) = G(a, \varphi_a).$$

Then we obtain

$$\begin{aligned} H^\omega(a) &= \lambda(a)\omega^2 - v(a) \\ &= \lambda(a)\omega^2 - G(a, \varphi_a) \\ &= \lambda(a)\omega^2 - \sum_{A \in S} \sum_{\sigma \in \Sigma} \lambda_{A,\sigma}(a) |\varphi_a(A) - \sigma|^2 \\ &= \lambda(a)\omega^2 - \sum_{A \in S} \sum_{\sigma \in \Sigma} \sum_{j=1}^{n} a_j \delta_\sigma^j(A) |\varphi_a(A) - \sigma|^2 \\ &= \sum_{j=1}^{n} a_j \left(\ell(\mathscr{C}_j)\omega^2 - \sum_{A \in S} \sum_{\sigma \in \Sigma} \delta_\sigma^j(A) |\varphi_a(A) - \sigma|^2 \right). \end{aligned}$$

Fix $j \in \mathbb{N}$ $(1 \leqslant j \leqslant n)$ and $a \in \mathbb{R}_+^n \setminus \{O\}$. We now show the following equality

$$\frac{\partial H^\omega}{\partial a_j}(a) = \ell(\mathscr{C}_j)\omega^2 - \sum_{A \in S} \sum_{\sigma \in \Sigma} \delta_\sigma^j(A) |\varphi_a(A) - \sigma|^2. \tag{14}$$

Indeed it suffices to show that for any $A \in S$, $g_A(a) = 0$, where $g_A(a)$ is defined by

$$\begin{aligned} g_A(a) &:= \sum_{k=1}^{n} a_k \sum_{\sigma \in \Sigma} \delta_\sigma^k(A) \frac{\partial}{\partial a_j} |\varphi_a(A) - \sigma|^2 \\ &= \sum_{\sigma \in \Sigma} \left(\sum_{k=1}^{n} a_k \delta_\sigma^k(A) \right) \frac{\partial}{\partial a_j} |\varphi_a(A) - \sigma|^2 \\ &= \sum_{\sigma \in \Sigma} \lambda_{A,\sigma}(a) \frac{\partial}{\partial a_j} |\varphi_a(A) - \sigma|^2. \end{aligned}$$

If $\lambda_A(a) = 0$, then for any $\sigma \in \Sigma$, we have $\lambda_{A,\sigma}(a) = 0$. Hence $g_A(a) = 0$. So we can concentrate our attention on the case $\lambda_A(a) \neq 0$.

For any fixed vertex $A \in S$, we define

$$x := \sum_{\sigma \in \Sigma} \lambda_{A,\sigma}(a)\sigma, \quad y := \sum_{\sigma \in \Sigma} \delta_\sigma^j(A)\sigma, \quad z := \lambda_A(a) \quad \text{and} \quad \delta := \sum_{\sigma \in \Sigma} \delta_\sigma^j(A).$$

Then we obtain $x = z\varphi_a(A)$, $\partial x/\partial a_j = y$ and $\partial z/\partial a_j = \delta$. Hence for any $\sigma \in \Sigma$, we have

$$\begin{aligned}
\frac{\partial}{\partial a_j}|\varphi_a(A)-\sigma|^2 &= \frac{\partial}{\partial a_j}(\varphi_a(A)-\sigma)(\overline{\varphi_a(A)-\sigma}) \\
&= 2\Re\left((\overline{\varphi_a(A)-\sigma})\frac{\partial}{\partial a_j}(\varphi_a(A)-\sigma)\right) \\
&= 2\Re\left(\left(\overline{\frac{x}{z}-\sigma}\right)\frac{\partial}{\partial a_j}\frac{x}{z}\right) \\
&= \frac{2}{z^3}\Re\left((\overline{x-z\sigma})\left(z\frac{\partial x}{\partial a_j}-x\frac{\partial z}{\partial a_j}\right)\right) \\
&= \frac{2}{z^3}\Re((\overline{x-z\sigma})(yz-x\delta)),
\end{aligned}$$

where for any $\zeta \in \mathbb{C}$, $\bar{\zeta}$ (resp. $\Re(\zeta)$) is the conjugate (resp. the real part) of z. So

$$\begin{aligned}
g_A(a) &= \sum_{\sigma\in\Sigma}\lambda_{A,\sigma}(a)\frac{\partial}{\partial a_j}|\varphi_a(A)-\sigma|^2 \\
&= \sum_{\sigma\in\Sigma}\lambda_{A,\sigma}(a)\frac{2}{z^3}\Re((\overline{x-z\sigma})(yz-x\delta)) \\
&= \frac{2}{z^3}\Re\left(\sum_{\sigma\in\Sigma}\lambda_{A,\sigma}(a)(\bar{x}yz-yz^2\bar{\sigma}-|x|^2\delta+xz\bar{\sigma}\delta)\right) \\
&= \frac{2}{z^3}\Re\left(\bar{x}yz^2-yz^2\left(\sum_{\sigma\in\Sigma}\lambda_{A,\sigma}(a)\bar{\sigma}\right)-|x|^2z\delta+xz\delta\left(\sum_{\sigma\in\Sigma}\lambda_{A,\sigma}(a)\bar{\sigma}\right)\right) \\
&= \frac{2}{z^3}\Re(\bar{x}yz^2-yz^2\bar{x}-|x|^2z\delta+xz\delta\bar{x}) \\
&= 0.
\end{aligned}$$

Keeping at heart all the conditions satisfied by the point a^ω, we have

$$\begin{aligned}
H^\omega(a^\omega) &= \lambda(a^\omega)\omega^2 - v(a^\omega) \\
&= \sum_{j=1}^{n} a_j^\omega\left(\ell(\mathscr{C}_j)\omega^2 - \sum_{A\in S}\sum_{\sigma\in\Sigma}\delta_\sigma^j(A)|\varphi_{a^\omega}(A)-\sigma|^2\right) \\
&= \sum_{j=1}^{n} a_j^\omega\frac{\partial H^\omega}{\partial a_j}(a^\omega) \\
&= 0
\end{aligned}$$

since for any $j \in \mathbb{N}$ $(1 \leqslant j \leqslant n)$, $a_j^\omega > 0$ implies $\partial H^\omega/\partial a_j(a^\omega) = 0$.

It remains to show that for any $a \in \mathbb{R}_+^n \setminus \{O\}$, we have $H^\omega(a) \geqslant 0$.

But by the properties of a^ω, we have

$$\sum_{j=1}^{n} \frac{\partial H^\omega}{\partial a_j}(a^\omega)(a_j - a_j^\omega) \geqslant 0$$

as for any $j \in \mathbb{N}$ $(1 \leqslant j \leqslant n)$, $\partial H^\omega/\partial a_j(a^\omega) \geqslant 0$ and if $a_j^\omega > a_j \geqslant 0$, then $\partial H^\omega/\partial a_j(a^\omega) = 0$. So it suffices to show the following inequality

$$H^\omega(a) \geqslant \sum_{j=1}^{n} \frac{\partial H^\omega}{\partial a_j}(a^\omega)(a_j - a_j^\omega) = \sum_{j=1}^{n} a_j \frac{\partial H^\omega}{\partial a_j}(a^\omega)$$

which is equivalent to say

$$G(a, \varphi_{a^\omega}) = \sum_{A \in S} \sum_{\sigma \in \Sigma} \lambda_{A,\sigma}(a) |\varphi_{a^\omega}(A) - \sigma|^2 \geqslant v(a).$$

But the last inequality is evident since by the definition of the function v, we have

$$v(a) = \inf_{\varphi \in \mathbb{C}^S} G(a, \varphi).$$

We have thus established our theorem. □

Remark. For any Σ-automaton $\mathscr{A}$, it seems difficult to give a similar algorithm to compute the general opacity $\omega_q(\mathscr{A})$ with $q \geqslant 1$. The difficulty is rather technical and consists principally in the fact that in general we do not have an explicit formula for the real valued function ψ defined on $\mathbb{R}_+^\Sigma$ by

$$\forall s = (s_\sigma)_{\sigma \in \Sigma} \in \mathbb{R}_+^\Sigma, \quad \psi(s) = \inf_{x \in \mathbb{C}} \sum_{\sigma \in \Sigma} s_\sigma |x - \sigma|^q.$$

Corollary 2. *For any finite automaton $\mathscr{A} = (S, i, \Sigma, t)$, the opacity $\omega(\mathscr{A})$ is algebraic over the field $\mathbb{Q}_\Sigma$ and its degree over $\mathbb{Q}_\Sigma$ is a power of* 2. *Here $\mathbb{Q}_\Sigma$ is the extension field of $\mathbb{Q}$ generated by the real numbers $|\sigma - \eta|^2$ $(\sigma, \eta \in \Sigma)$.*

Proof. Put $\omega = \omega(\mathscr{A})$ and denote by $\mathscr{C}_1, \mathscr{C}_2, \ldots, \mathscr{C}_n$ the simple circuits of $\mathscr{A}$. Then by Theorem 2, we can find a point $a^\omega = (a_j^\omega)_{1 \leqslant j \leqslant n} \in \mathbb{R}_+^n \setminus \{O\}$ such that for any $j \in \mathbb{N}$ $(1 \leqslant j \leqslant n)$, we have $\partial H^\omega/\partial a_j(a^\omega) \geqslant 0$ and if $a_j^\omega > 0$, then $\partial H^\omega/\partial a_j(a^\omega) = 0$. Hence if $j \in \mathbb{N}$ $(1 \leqslant j \leqslant n)$ verifies $\partial H^\omega/\partial a_j(a^\omega) > 0$, we have necessarily $a_j^\omega = 0$. In this case the circuit $\mathscr{C}_j$ does not contribute to the value of ω and we can ignore it. Suppose that we have suppressed all these useless simple circuits. Without loss of generality, we denote still the remaining simple circuits by $\mathscr{C}_1, \mathscr{C}_2, \ldots, \mathscr{C}_n$. Then the real number ω satisfies the following system of equations

$$\frac{\partial H^\omega}{\partial a_j}(a^\omega) = 0 \ (1 \leqslant j \leqslant n).$$

But by Relation (14) and the definition of φ_a, we see that $\partial H^\omega/\partial a_j$ is a polynomial of degree 2 with coefficients in $\mathbb{Q}_\Sigma$ and variables ω and $\lambda_{A,\sigma}(a)/\lambda_A(a)$ $(A \in S,\ \sigma \in \Sigma$ and $a \in \mathbb{R}_+^n \setminus \{O\})$. So the real numbers ω and $\lambda_{A,\sigma}(a^\omega)/\lambda_A(a^\omega)$ $(A \in S$ and $\sigma \in \Sigma)$ should

satisfy a system of algebraic equations of degree 2 with coefficients in $\mathbb{Q}_\Sigma$. Thus ω is algebraic over $\mathbb{Q}_\Sigma$ and its degree over this field is a power of 2. □

Remark. In general, neither $\omega(\mathscr{A})$ nor $(\omega(\mathscr{A}))^2$ is rational. In fact, as we shall show later in Section 9 that even if $\mathbb{Q}_\Sigma = \mathbb{Q}$, the number $(\omega(\mathscr{A}))^2$ may not be rational.

6. An important formula for $\omega(\mathscr{A})$

To some extent, a finite automaton $\mathscr{A}$ is determined by its simple circuits. So is its opacity $\omega(\mathscr{A})$. Formula (10) has already implicitly confirmed this point. However, we can do better by giving below a more direct relationship. The reader can also consult [1] for the general case $\omega_q(\mathscr{A})$, where we have given a quite different proof.

Theorem 3. *Let $\mathscr{A} = (S, i, \Sigma, t)$ be a finite automaton and $\mathscr{C}_1, \mathscr{C}_2, \ldots, \mathscr{C}_n$ be its simple circuits. Then we have*

$$\omega(\mathscr{A}) = \min_{\varphi \in \mathbb{C}^S} \max_{1 \leqslant j \leqslant n} \left(\frac{1}{\ell(\mathscr{C}_j)} \sum_{A \in S} \sum_{\sigma \in \Sigma} \delta_\sigma^j(A) |\varphi(A) - \sigma|^2 \right)^{1/2}. \tag{15}$$

Proof. Let $\mathscr{C}$ be a circuit on the graph of the finite automaton $\mathscr{A}$. Then there exists a point $a(\mathscr{C}) = (a_1(\mathscr{C}), a_2(\mathscr{C}), \ldots, a_n(\mathscr{C}))$ in $\mathbb{N}^n \setminus \{O\}$ such that

$$\mathscr{C} = \sum_{j=1}^{n} a_j(\mathscr{C}) \mathscr{C}_j.$$

Hence by Relations (3)–(5), we have, for any complex valued function φ defined on S, the following inequality

$$\begin{aligned} \frac{G(a(\mathscr{C}), \varphi)}{\lambda(a(\mathscr{C}))} &= \frac{\sum_{A \in S} \sum_{\sigma \in \Sigma} \sum_{j=1}^{n} a_j(\mathscr{C}) \delta_\sigma^j(A) |\varphi(A) - \sigma|^2}{\sum_{j=1}^{n} a_j(\mathscr{C}) \ell(\mathscr{C}_j)} \\ &= \frac{\sum_{j=1}^{n} a_j(\mathscr{C}) (\sum_{A \in S} \sum_{\sigma \in \Sigma} \delta_\sigma^j(A) |\varphi(A) - \sigma|^2)}{\sum_{j=1}^{n} a_j(\mathscr{C}) \ell(\mathscr{C}_j)} \\ &\leqslant \max_{1 \leqslant j \leqslant n} \frac{1}{\ell(\mathscr{C}_j)} \sum_{A \in S} \sum_{\sigma \in \Sigma} \delta_\sigma^j(A) |\varphi(A) - \sigma|^2. \end{aligned} \tag{16}$$

Thus from Formula (10), we deduce

$$\omega(\mathscr{A}) \leqslant \inf_{\varphi \in \mathbb{C}^S} \max_{1 \leqslant j \leqslant n} \left(\frac{1}{\ell(\mathscr{C}_j)} \sum_{A \in S} \sum_{\sigma \in \Sigma} \delta_\sigma^j(A) |\varphi(A) - \sigma|^2 \right)^{1/2}. \tag{17}$$

Now set $\omega = \omega(\mathscr{A})$. By Theorem 2, we can find a point $a^\omega = (a_1^\omega, \ldots, a_n^\omega)$ in $\mathbb{R}_+^n \setminus \{O\}$ such that for any $j \in \mathbb{N}$ $(1 \leqslant j \leqslant n)$, we have $\partial H^\omega / \partial a_j(a^\omega) \geqslant 0$. Then for any

integer j $(1 \leqslant j \leqslant n)$, we deduce from Relation (14) the following inequality

$$\omega^2 \geqslant \frac{1}{\ell(\mathscr{C}_j)} \sum_{A \in S} \sum_{\sigma \in \Sigma} \delta_\sigma^j(A) |\varphi_{a^\omega}(A) - \sigma|^2.$$

Consequently we obtain

$$\omega(\mathscr{A}) \geqslant \max_{1 \leqslant j \leqslant n} \left(\frac{1}{\ell(\mathscr{C}_j)} \sum_{A \in S} \sum_{\sigma \in \Sigma} \delta_\sigma^j(A) |\varphi_{a^\omega}(A) - \sigma|^2 \right)^{1/2}$$

$$\geqslant \inf_{\varphi \in \mathbb{C}^S} \max_{1 \leqslant j \leqslant n} \left(\frac{1}{\ell(\mathscr{C}_j)} \sum_{A \in S} \sum_{\sigma \in \Sigma} \delta_\sigma^j(A) |\varphi(A) - \sigma|^2 \right)^{1/2}. \tag{18}$$

Combing Relations (17) and (18), we gain the equality

$$\omega(\mathscr{A}) = \max_{1 \leqslant j \leqslant n} \left(\frac{1}{\ell(\mathscr{C}_j)} \sum_{A \in S} \sum_{\sigma \in \Sigma} \delta_\sigma^j(A) |\varphi_{a^\omega}(A) - \sigma|^2 \right)^{1/2}$$

$$= \inf_{\varphi \in \mathbb{C}^S} \max_{1 \leqslant j \leqslant n} \left(\frac{1}{\ell(\mathscr{C}_j)} \sum_{A \in S} \sum_{\sigma \in \Sigma} \delta_\sigma^j(A) |\varphi(A) - \sigma|^2 \right)^{1/2}$$

which is an equivalent form of our theorem. □

Corollary 3. *Let $\mathscr{I}_\Sigma$ be a Σ-automaton having only one state. Then*

$$\omega(\mathscr{I}_\Sigma) = \min_{x \in \mathbb{C}} \max_{\sigma \in \Sigma} |x - \sigma|.$$

Proof. We need only remark that the length of a simple circuit of $\mathscr{I}_\Sigma$ equals 1. □

7. Another proof of the equality $\omega(\mathscr{A}) = \Omega(\mathscr{A})$

In this section we shall give another proof of the equality $\omega(\mathscr{A}) = \Omega(\mathscr{A})$ which was already established in a more general setting in [7,8]. The reader can also consult [4] for a third proof.

We begin with a lemma.

Lemma. *Let $\mathscr{A} = (S, i, \Sigma, t)$ be a finite automaton and φ be a complex valued function defined on S. Then for any sequence of labels ε, we can find a family of ultimately periodic sequences $(\varepsilon^{(j)})_{j \geqslant 0}$ (depending on φ and on ε) such that*

$$||\varphi(\mathscr{A}\varepsilon) - \varepsilon|| = \lim_{j \to \infty} ||\varphi(\mathscr{A}\varepsilon^{(j)}) - \varepsilon^{(j)}||.$$

Proof. Let $\varepsilon = (\varepsilon(m))_{m\geqslant 0}$ be an infinite sequence of labels. Then we can find an increasing sequence of integers $(k_j)_{j\geqslant 0}$ depending perhaps on ε and on φ such that

$$||\varphi(\mathscr{A}\varepsilon) - \varepsilon||^2 = \lim_{j\to\infty} \frac{1}{k_j} \sum_{m=0}^{k_j-1} |\varphi((\mathscr{A}\varepsilon)(m)) - \varepsilon(m)|^2. \tag{19}$$

For any $j \in \mathbb{N}$, denote by $\mathscr{P}_j$ the path on $\mathscr{A}$ generated by the sequence $(\varepsilon(m))_{0\leqslant m<k_j}$. Then $\mathscr{P}_j$ is the first part of $\mathscr{P}(\varepsilon)$ (which is the infinite path on $\mathscr{A}$ generated by ε) composed of k_j arrows. Let $S(\mathscr{P})$ be the set of all vertices appearing in $\mathscr{P}$ for an infinite number of times. Since S is a finite set, there exists $l \in \mathbb{N}$ such that for any $m \in \mathbb{N}$ $(m \geqslant l)$, we have $t(i, \varepsilon(0)\cdots\varepsilon(m)) \in S(\mathscr{P})$, i.e., from the rank l, the arrows of $\mathscr{P}$ move between the vertices in $S(\mathscr{P})$. Put $A = t(i, \varepsilon(0)\cdots\varepsilon(l))$. Now that $\mathscr{A}$ contains only $s := Card(S) \times Card(\Sigma)$ arrows on the whole and the path $\mathscr{P}$ passes the vertex A for an infinite number of times, thus for any $m \in \mathbb{N}$ $(m > l+1)$, we can find a finite path of length shorter than s linking $t(i, \varepsilon(0)\cdots\varepsilon(m-1))$ to A, i.e., we can find a finite word $\sigma^{(m)}$ over Σ of length shorter than s such that $A = t(i, \varepsilon(0)\cdots\varepsilon(m-1)\sigma^{(m)})$. In particular, for any $j \in \mathbb{N}$ $(k_j > l+1)$, we can find $\sigma^{(k_j)} = (\sigma^{(k_j)}(m))_{m\geqslant 0}$ of length $\leqslant s$ such that $A = t(i, \varepsilon(0)\cdots\varepsilon(k_j-1)\sigma^{(k_j)})$. So $A = t(A, \varepsilon(l+1)\cdots\varepsilon(k_j-1)\sigma^{(k_j)})$ and the word $\varepsilon(l+1)\cdots\varepsilon(k_j-1)\sigma^{(k_j)}$ defines a circuit $\mathscr{C}^{(j)}$ with A as its starting-point. Then there exists an ultimately periodic sequence of labels $\varepsilon^{(j)}$ such that the infinite path $\mathscr{P}(\varepsilon^{(j)})$ generated by $\varepsilon^{(j)}$ ultimately winds up on $\mathscr{C}^{(j)}$. Denote by $|\sigma^{(k_j)}|$ the length of $\sigma^{(k_j)}$. Then $|\sigma^{(k_j)}| \leqslant s$ and by Relations (19) and (9), we have

$$\begin{aligned}
&||\varphi(\mathscr{A}\varepsilon) - \varepsilon||^2 \\
&\quad= \lim_{j\to\infty} \frac{1}{k_j} \left(\sum_{m=l+1}^{k_j-1} |\varphi((\mathscr{A}\varepsilon)(m)) - \varepsilon(m)|^2 \right. \\
&\qquad \left. + \sum_{m=0}^{|\sigma^{(k_j)}|-1} |\varphi(t((\mathscr{A}\varepsilon)(k_j-1), \sigma^{(k_j)}(0)\cdots\sigma^{(k_j)}(m))) - \sigma^{(k_j)}(m)|^2 \right) \\
&\quad= \lim_{j\to\infty} \frac{G(a(\mathscr{C}^{(j)}), \varphi)}{\lambda(a(\mathscr{C}^{(j)}))} \\
&\quad= \lim_{j\to\infty} ||\varphi(\mathscr{A}\varepsilon^{(j)}) - \varepsilon^{(j)}||^2
\end{aligned}$$

which is just our lemma. □

Remark. We can ask whether this lemma may follow from general consideration of continuity. However although the set of ultimately periodic sequences is dense in $\Sigma^{\mathbb{N}}$ for the canonical product topology, the function $\varepsilon \to ||\varphi(\mathscr{A}\varepsilon) - \varepsilon||$ $(\varphi \in \mathbb{C}^S)$ may be not continuous for this topology. Consider for example the Ising automaton $\mathscr{A}_0$ defined in Fig. 1 (see Section 9). Let ε be the constant sequence of common value 1. Then $||\varphi_0(\mathscr{A}_0\varepsilon) - \varepsilon|| = 1$. Let $j \in \mathbb{N}$ and $\varepsilon_j(j) = -1$. For any $m \in \mathbb{N}$ with $m \neq j$, define

$\varepsilon_j(m) = 1$. Put $\varepsilon_j = (\varepsilon_j(m))_{m \geqslant 0}$. Clearly the family of sequences $(\varepsilon_j)_{j \geqslant 0}$ tends towards ε. But for any $j \in \mathbb{N}$, we have $||\varphi_0(\mathscr{A}_0 \varepsilon_j) - \varepsilon_j|| = 3$.

Theorem 4. *For any finite automaton $\mathscr{A} = (S, i, \Sigma, t)$, we have*

$$\omega(\mathscr{A}) = \Omega(\mathscr{A}).$$

Proof. Let φ be a complex valued function defined on S and $\varepsilon = (\varepsilon(m))_{m \geqslant 0}$ be an infinite sequence of labels. Then by lemma above, we can find a family of ultimately periodic sequences $(\varepsilon^{(j)})_{j \geqslant 0}$ (depending on φ and on ε) such that

$$||\varphi(\mathscr{A}\varepsilon) - \varepsilon|| = \lim_{j \to \infty} ||\varphi(\mathscr{A}\varepsilon^{(j)}) - \varepsilon^{(j)}||.$$

Let $\mathscr{C}_1, \mathscr{C}_2, \ldots, \mathscr{C}_n$ be the simple circuits of $\mathscr{A}$. For any $j \in \mathbb{N}$, since the sequence of labels $\varepsilon^{(j)}$ is ultimately periodic, then there exists a circuit $\mathscr{C}^{(j)}$ of $\mathscr{A}$ such that the infinite path $\mathscr{P}(\varepsilon^{(j)})$ generated by $\varepsilon^{(j)}$ ultimately winds up on $\mathscr{C}^{(j)}$. Thus we can find a point $a(\mathscr{C}^{(j)}) = (a_k(\mathscr{C}^{(j)}))_{1 \leqslant k \leqslant n} \in \mathbb{N}^n \setminus \{O\}$ such that $\mathscr{C}^{(j)} = \sum_{k=1}^{n} a_k(\mathscr{C}^{(j)}) \mathscr{C}_k$. Hence by Relations (8) and (16), we have

$$\begin{aligned} ||\varphi(\mathscr{A}\varepsilon) - \varepsilon||^2 &= \lim_{j \to \infty} ||\varphi(\mathscr{A}\varepsilon^{(j)}) - \varepsilon^{(j)}||^2 \\ &= \lim_{j \to \infty} \frac{G(a(\mathscr{C}^{(j)}), \varphi)}{\lambda(a(\mathscr{C}^{(j)}))} \\ &\leqslant \max_{1 \leqslant k \leqslant n} \frac{1}{\ell(\mathscr{C}_k)} \sum_{A \in S} \sum_{\sigma \in \Sigma} \delta_\sigma^k(A) |\varphi(A) - \sigma|^2 \end{aligned} \tag{20}$$

which implies immediately, with the help of Theorem 3, the following inequality

$$\begin{aligned} \Omega(\mathscr{A}) &= \sup_{\varepsilon \in \Sigma^{\mathbb{N}}} \inf_{\varphi \in \mathbb{C}^S} ||\varphi(\mathscr{A}\varepsilon) - \varepsilon|| \\ &\leqslant \inf_{\varphi \in \mathbb{C}^S} \max_{1 \leqslant k \leqslant n} \left(\frac{1}{\ell(\mathscr{C}_k)} \sum_{A \in S} \sum_{\sigma \in \Sigma} \delta_\sigma^k(A) |\varphi(A) - \sigma|^2 \right)^{1/2} \\ &= \omega(\mathscr{A}). \end{aligned}$$

Consequently we have $\Omega(\mathscr{A}) = \omega(\mathscr{A})$ for $\Omega(\mathscr{A}) \geqslant \omega(\mathscr{A})$ holds trivially. □

By the way, we have also obtained a new proof of the following theorem which is a special case of Corollary 2 in [8].

Theorem 5. *For any finite automaton $\mathscr{A} = (S, i, \Sigma, t)$, we have*

$$\Omega(\mathscr{A}) = \inf_{\varphi \in \mathbb{C}^S} \sup_{\varepsilon \in \Sigma^{\mathbb{N}}} ||\varphi(\mathscr{A}\varepsilon) - \varepsilon||.$$

Proof. Let $\mathscr{C}_1, \mathscr{C}_2, \ldots, \mathscr{C}_n$ be the simple circuits of $\mathscr{A}$. Then by Relation (20), we have, for any $\varepsilon \in \Sigma^{\mathbb{N}}$ and $\varphi \in \mathbb{C}^S$, the following inequality

$$||\varphi(\mathscr{A}\varepsilon) - \varepsilon|| \leqslant \max_{1 \leqslant k \leqslant n} \left(\frac{1}{\ell(\mathscr{C}_k)} \sum_{A \in S} \sum_{\sigma \in \Sigma} \delta_\sigma^k(A) |\varphi(A) - \sigma|^2 \right)^{1/2}.$$

As a result, we obtain, with the help of Theorems 3 and 4, the inequality

$$\begin{aligned} &\inf_{\varphi \in \mathbb{C}^S} \sup_{\varepsilon \in \Sigma^{\mathbb{N}}} ||\varphi(\mathscr{A}\varepsilon) - \varepsilon|| \\ &\quad \leqslant \inf_{\varphi \in \mathbb{C}^S} \max_{1 \leqslant k \leqslant n} \left(\frac{1}{\ell(\mathscr{C}_k)} \sum_{A \in S} \sum_{\sigma \in \Sigma} \delta_\sigma^k(A) |\varphi(A) - \sigma|^2 \right)^{1/2} \\ &\quad = \Omega(\mathscr{A}). \end{aligned}$$

On the other hand, from the definition of $\Omega(\mathscr{A})$, we have trivially

$$\inf_{\varphi \in \mathbb{C}^S} \sup_{\varepsilon \in \Sigma^{\mathbb{N}}} ||\varphi(\mathscr{A}\varepsilon) - \varepsilon|| \geqslant \Omega(\mathscr{A}).$$

We have thus finished the proof of our theorem. □

8. An existence theorem

Let $\mathscr{A} = (S, i, \Sigma, t)$ be a finite automaton. From the definition of $\omega(\mathscr{A})$, it is natural to ask whether there exists an ultimately periodic sequence of labels ε such that

$$\omega(\mathscr{A}) = \inf_{\varphi \in \mathbb{C}^S} ||\varphi(\mathscr{A}\varepsilon) - \varepsilon||. \tag{21}$$

If the answer were positive, then by Formulas (8), (5) and (6), the number $(\omega(\mathscr{A}))^2$ should be in $\mathbb{Q}_\Sigma$, thus a rational number if all the numbers $|\sigma - \eta|^2$ $(\sigma, \eta \in \Sigma)$ are rational (see our remark about Corollary 2). In Section 9 we shall show that $\omega(\mathscr{A})$ may be not rational even if Σ is a subset of $\mathbb{Q}$ (see also [7,4]). Hence in general, we cannot find an ultimately periodic sequence of labels ε satisfying Equality (21). In other words, in general the sup in the definition of $\omega(\mathscr{A})$ cannot be attained. By using Theorem 3, we shall show below that the sup in the definition of $\Omega(\mathscr{A})$ can be attained (see also [7,1]). However, such a difference between Ω and ω is only apparent and does not contradict the fact $\Omega = \omega$.

Theorem 6. *For any finite automaton $\mathscr{A} = (S, i, \Sigma, t)$, there exists an infinite sequence of labels $\varepsilon \in \Sigma^{\mathbb{N}}$ such that we have*

$$\Omega(\mathscr{A}) = \inf_{\varphi \in \mathbb{C}^S} ||\varphi(\mathscr{A}\varepsilon) - \varepsilon||.$$

Proof. We shall adopt the improved version of the construction method discovered firstly by Loraud (cf. [4]) to construct an infinite sequence of labels ε satisfying our theorem (see also [7,8]).

Let $\mathscr{C}_1, \mathscr{C}_2, \ldots, \mathscr{C}_n$ be the simple circuits of the finite automaton $\mathscr{A}$. For any two integers j,k $(1 \leqslant j < k \leqslant n)$, we say that they are equivalent if there exists a circuit $\mathscr{C}$ on $\mathscr{A}$ which contains $\mathscr{C}_j$ and $\mathscr{C}_k$. In other words, on the graph of $\mathscr{A}$, we can pass from $\mathscr{C}_j$ to $\mathscr{C}_k$ and conversely. In this way we have defined an equivalence relation over the set of integers $\{1,2,\ldots, n\}$. Denote by $C^{(1)}, C^{(2)}, \ldots, C^{(d)}$ the equivalence classes. For each $m \in \mathbb{N}$ $(1 \leqslant m \leqslant d)$ and $\varphi \in \mathbb{C}^S$, define

$$I_m(\varphi) = \max_{j \in C^{(m)}} \left(\frac{1}{\ell(\mathscr{C}_j)} \sum_{A \in S} \sum_{\sigma \in \Sigma} \delta_\sigma^j(A) |\varphi(A) - \sigma|^2 \right)^{1/2} \quad \text{and} \quad J_m = \inf_{\phi \in \mathbb{C}^S} I_m(\phi).$$

It is clear that for any two integers j,k $(1 \leqslant j < k \leqslant n)$, if they are not equivalent, the simple circuits $\mathscr{C}_j$ and $\mathscr{C}_k$ have not any common vertex. Thus we have

$$\inf_{\varphi \in \mathbb{C}^S} \max_{1 \leqslant m \leqslant d} I_m(\varphi) = \max_{1 \leqslant m \leqslant d} \inf_{\varphi \in \mathbb{C}^S} I_m(\varphi).$$

Then from Theorems 3 and 4, we deduce

$$\begin{aligned} \Omega(\mathscr{A}) &= \inf_{\varphi \in \mathbb{C}^S} \max_{1 \leqslant j \leqslant n} \left(\frac{1}{\ell(\mathscr{C}_j)} \sum_{A \in S} \sum_{\sigma \in \Sigma} \delta_\sigma^j(A) |\varphi(A) - \sigma|^2 \right)^{1/2} \\ &= \inf_{\varphi \in \mathbb{C}^S} \max_{1 \leqslant m \leqslant d} I_m(\varphi) \\ &= \max_{1 \leqslant m \leqslant d} \inf_{\varphi \in \mathbb{C}^S} I_m(\varphi) \\ &= \max_{1 \leqslant m \leqslant d} J_m. \end{aligned}$$

Hence we can find an integer m $(1 \leqslant m \leqslant d)$ such that $\Omega(\mathscr{A}) = J_m$. Without loss of generality, we can also suppose $C^{(m)} = \{1,2,\ldots,k\}$.

Now we do our construction by recurrence.

Step 1: Since $\mathscr{A}$ is connected, there exists a finite sequence of labels ε_1 such that the path on $\mathscr{A}$ generated by ε_1 contains $\mathscr{C}_1$. But the integers 1 and 2 are in the same class $C^{(m)}$, so we can find a finite sequence σ_1 such that the path generated by $\varepsilon_1\sigma_1$ meets $\mathscr{C}_2$. Circulating $[\exp(|\varepsilon_1\sigma_1|)]$ times on $\mathscr{C}_2$, we obtain a finite sequence $\varepsilon_1\sigma_1\varepsilon_2$. In the same way, we can also find a finite sequence σ_2 such that the path generated by $\varepsilon_1\sigma_1\varepsilon_2\sigma_2$ meets $\mathscr{C}_3$. Circulating $[\exp(|\varepsilon_1\sigma_1\varepsilon_2\sigma_2|)]$ times on $\mathscr{C}_3$, we get $\varepsilon_1\sigma_1\varepsilon_2\sigma_2\varepsilon_3$. Continue this procedure until all the k simple circuits $\mathscr{C}_1, \mathscr{C}_2, \ldots, \mathscr{C}_k$ have been visited and we are now on $\mathscr{C}_1$. We obtain thus a finite sequence $\varepsilon^{(1)}$ which describes the preceding path thus constructed.

Step j $(j \geqslant 2)$: Assume that we have constructed the finite sequence $\varepsilon^{(j-1)}$. Following this sequence, we arrive again on $\mathscr{C}_1$. Circulating $[\exp(|\varepsilon^{(j-1)}|)]$ times on $\mathscr{C}_1$, we get $\varepsilon^{(j-1)}\varepsilon_1^{(j)}$. Then repeat Step 1 and we obtain a finite sequence $\varepsilon^{(j)}$.

It is clear that the family of finite sequences $(\varepsilon^{(j)})_{j \geqslant 1}$ converges in the usual sense to an infinite sequence ε. Furthermore by our construction and the definition of the semi-norm $||\cdot||$, we have, for any complex valued function φ defined on S,

$$||\varphi(\mathscr{A}\varepsilon) - \varepsilon|| \geqslant I_m(\varphi) = \max_{j \in C^{(m)}} \left(\frac{1}{\ell(\mathscr{C}_j)} \sum_{A \in S} \sum_{\sigma \in \Sigma} \delta_\sigma^j(A) |\varphi(A) - \sigma|^2 \right)^{1/2}$$

since $x\exp(-x)$ goes to zero when $x \to +\infty$. Consequently

$$\Omega(\mathscr{A}) = J_m \leqslant \inf_{\varphi \in \mathbb{C}^S} ||\varphi(\mathscr{A}\varepsilon) - \varepsilon||_q$$

from which we conclude immediately our theorem. □

9. Application to the inhomogeneous Ising chain

Since the discovery of quasicrystals, it was realized that one can apply automata theory in theoretical physics to describe some nonperiodic but ordered phenomena. A typical example is the inhomogeneous Ising chain which contains $N+1$ particles of spins $\pm$ ranged on a line. For any $q \in \mathbb{N}$ $(0 \leqslant q \leqslant N)$, denote by $\sigma(q)$ the spin of the qth particle. A configuration is a finite sequence of spins $\sigma = (\sigma(q))_{0 \leqslant q \leqslant N}$. Let $\varepsilon \in \{-1,+1\}^N$ be a finite sequence of $\pm$ which represents for example the distribution of two different substances or some impurities in an alloy. The system's Hamiltonian at the configuration σ is defined as

$$\mathscr{H}_\varepsilon(\sigma) = -J \sum_{q=0}^{N-1} \varepsilon(q)\sigma(q)\sigma(q+1) - H \sum_{q=0}^{N} \sigma(q),$$

where $J > 0$ is the coupling constant and $H \geqslant 0$ is the external magnetic field.

Given parameters J and H, an important problem in statistical mechanics is to determine the system's equilibrium state, i.e., the configuration $\hat{\sigma}$ which minimizes the Hamiltonian $\mathscr{H}_\varepsilon(\sigma)$. Let $\hat{\sigma}$ be an equilibrium configuration. Kamae and Mendès France showed that $\hat{\sigma}$ should satisfy the recurrence relation (cf. [3]):

$$\hat{\sigma}(q) = \operatorname{sgn}(\delta(q) + 2\varepsilon(q)\hat{\sigma}(q+1)) \quad \text{for } 0 \leqslant q < N \quad \text{and} \quad \hat{\sigma}(N) = \operatorname{sgn}(\delta(N)),$$

where the finite sequence $\delta = (\delta(q))_{0 \leqslant q \leqslant N}$ is defined by

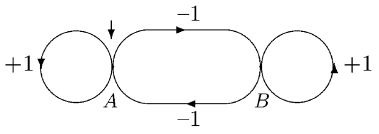
$$\delta(q+1) = \alpha + \varepsilon(q)\operatorname{sgn}(\delta(q))\min\{2, |\delta(q)|\} \quad (0 \leqslant q < N)$$

with $\alpha = 2H/J$ and $\delta(0)$ fixed beforehand (by convention $\operatorname{sgn}(0)$ can take here the two values $+1$ and -1 arbitrarily. This corresponds to the fact that there are probably more than one equilibrium states under the same conditions). We shall restrict our attention to the case $\delta(0) = \alpha + 2$. Then the study of our system is reduced to that of the following recurrence relation:

$$\begin{cases} \delta(0) = \alpha + 2, \\ \delta(q+1) = \alpha + \varepsilon(q)\operatorname{sgn}(\delta(q))\min\{2, |\delta(q)|\}. \end{cases} \tag{22}$$

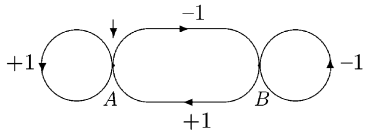
The finite sequence δ which depends on α and on ε will be denoted by $\delta^\alpha(\varepsilon)$. It was shown in [3,5] that the mapping $\varepsilon \mapsto \delta^\alpha(\varepsilon)$, defined from $\{-1,+1\}^*$ to S_α^* where S_α is a finite subset of $[\alpha-2, \alpha+2]$, is given by a finite automaton with output function $(\mathscr{A}_\alpha, \psi_\alpha)$, i.e., for any $\varepsilon \in \{-1,+1\}^*$ and any $q \in \mathbb{N}$ $(1 \leqslant q \leqslant N)$, we have $\delta^\alpha(\varepsilon)(q) = \psi_\alpha(t_\alpha(i_\alpha, \varepsilon(0)\cdots\varepsilon(q-1)))$ where i_α (resp. t_α) is the initial state (resp. the transition function) of $\mathscr{A}_\alpha$.

For $\alpha = 0$, Relation (22) gives $\delta(q+1) = 2\varepsilon(0)\varepsilon(1)\cdots\varepsilon(q)$ and we obtain the finite automaton with output function defined in Fig. 1.



$$\psi_0(A) = +2 \quad \text{and} \quad \psi_0(B) = -2$$

Fig. 1. Ising automaton $\mathscr{A}_0$.



$$\psi_\alpha(A) = \alpha + 2 \quad \text{and} \quad \psi_\alpha(B) = \alpha - 2$$

Fig. 2. Ising automaton $\mathscr{A}_\alpha$ with $\alpha \geqslant 4$.

If $\alpha \geqslant 4$, Relation (22) becomes $\delta(q+1) = \alpha + 2\varepsilon(q)$ and the finite automaton with output function given by Fig. 2 satisfies our need.

If $0 < \alpha < 4$, according to the nature of $4/\alpha$, we obtain two types of finite automata with output function (see Figs. 3 and 4). In order to distinguish them, we denote the Ising automaton $\mathscr{A}_\alpha$ by $\mathscr{N}_\mu$ or $\mathscr{L}_\mu$ if $4/\alpha \in \mathbb{N}$ or not where $\mu = \lfloor 4/\alpha \rfloor$ is the integral part of $4/\alpha$.

Now $\Sigma = \{+1, -1\}$ and $\omega(\mathscr{I}_\Sigma) = 1$. Denote by n_α the number of simple circuits of the Ising automaton $\mathscr{A}_\alpha$ (of course here we need not distinguish simple circuits which are different only in their points of base. See Section 4 for related discussions). Then for any point $a \in \mathbb{R}_+^{n_\alpha} \setminus \{O\}$ and any $C \in S_\alpha$, we have

$$G_C(a) = \frac{4\lambda_{C,+1}(a)\lambda_{C,-1}(a)}{\lambda_C(a)}.$$

Thus we obtain, for any positive number ω and any point $a \in \mathbb{R}_+^{n_\alpha} \setminus \{O\}$,

$$H^\omega(a) = \lambda(a)\omega^2 - \sum_{C \in S_\alpha} \frac{4\lambda_{C,+1}(a)\lambda_{C,-1}(a)}{\lambda_C(a)}. \tag{23}$$

Since we have four types of Ising automata, below we shall distinguish four cases to compute $\omega^{(\alpha)} := \omega(\mathscr{A}_\alpha)$ by using the algorithm given in Theorem 2.

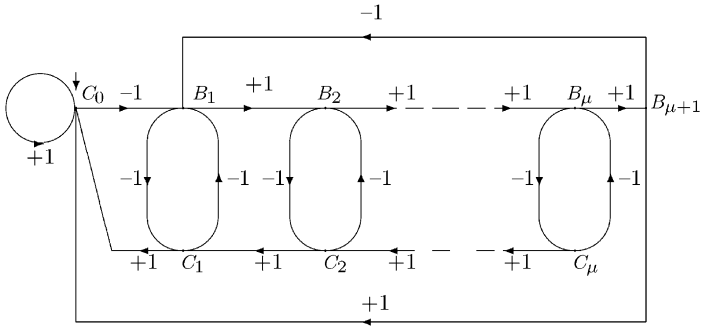
Case 1: $\alpha = 0$. In this case we have $n_0 = 3$ (see Fig. 5).

For any point $a = (a_1, a_2, a_3) \in \mathbb{R}_+^3 \setminus \{O\}$, we have

$$\lambda_{A,+1}(a) = a_1, \quad \lambda_{A,-1}(a) = a_2 \quad \text{and} \quad \lambda_{B,+1}(a) = a_3, \quad \lambda_{B,-1}(a) = a_2.$$

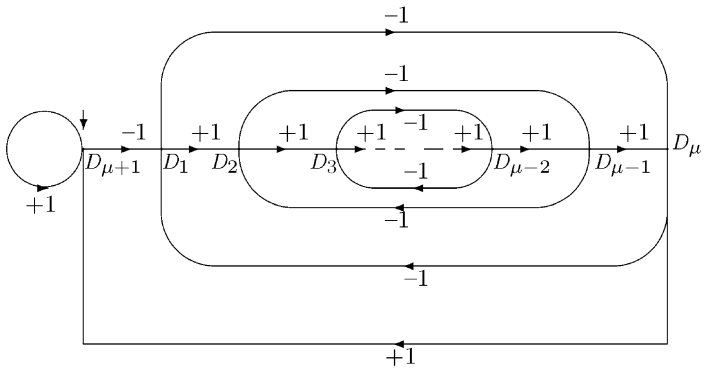
Hence for any positive number ω, we have

$$H^\omega(a) = (a_1 + 2a_2 + a_3)\omega^2 - \frac{4a_1a_2}{a_1 + a_2} - \frac{4a_2a_3}{a_2 + a_3}$$



$$\psi_\alpha(B_j) = j\alpha - 2 \text{ and } \psi_\alpha(C_j) = 2 - (j-1)\alpha \text{ with } 4/\alpha \notin \mathbb{N}$$

Fig. 3. Ising automaton $\mathscr{A}_\alpha$ (noted $\mathscr{L}_\mu$).



$$\psi_\alpha(D_j) = j\alpha - 2 \text{ with } 4/\alpha \in \mathbb{N}$$

Fig. 4. Ising automaton $\mathscr{A}_\alpha$ (noted $\mathscr{N}_\mu$).

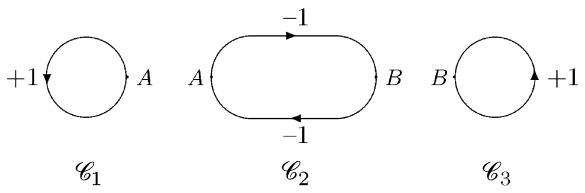


Fig. 5. Simple circuits of $\mathscr{A}_0$.

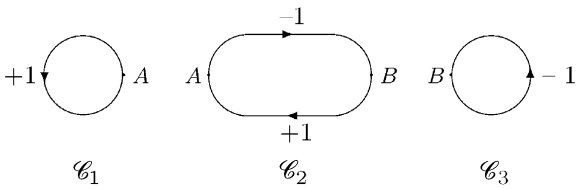


Fig. 6. Simple circuits of $\mathscr{A}_\alpha$ with $\alpha \geqslant 4$.

from which we obtain

$$\frac{\partial H^\omega}{\partial a_1}(a) = \omega^2 - \frac{4a_2^2}{(a_1+a_2)^2},$$

$$\frac{\partial H^\omega}{\partial a_2}(a) = 2\omega^2 - \frac{4a_1^2}{(a_1+a_2)^2} - \frac{4a_3^2}{(a_2+a_3)^2},$$

$$\frac{\partial H^\omega}{\partial a_3}(a) = \omega^2 - \frac{4a_2^2}{(a_2+a_3)^2}.$$

Then we put

$$\frac{\partial H^\omega}{\partial a_1}(a) = \frac{\partial H^\omega}{\partial a_2}(a) = \frac{\partial H^\omega}{\partial a_3}(a) = 0$$

and we obtain $\omega = 1$, i.e., $\omega^{(0)} = 1$. So $\mathscr{A}_0$ is opaque (see also [5] and [8]).

Case 2: $\alpha \geqslant 4$. In this case we also have $n_\alpha = 3$ (see Fig. 6).

For any point $a = (a_1, a_2, a_3) \in \mathbb{R}^3_+ \setminus \{O\}$, we have

$$\lambda_{A,+1}(a) = a_1 + a_2, \quad \lambda_{A,-1}(a) = 0 \quad \text{and} \quad \lambda_{B,+1}(a) = 0,\ \lambda_{B,-1}(a) = a_2 + a_3.$$

Hence for any positive number ω, the auxiliary function H^ω takes the form

$$H^\omega(a) = (a_1 + 2a_2 + a_3)\omega^2$$

and we obtain, by taking the weak partial derivatives of H^ω,

$$\frac{\partial H^\omega}{\partial a_1}(a) = \omega^2,$$

$$\frac{\partial H^\omega}{\partial a_2}(a) = 2\omega^2,$$

$$\frac{\partial H^\omega}{\partial a_3}(a) = \omega^2.$$

Then from the following system of equations

$$\frac{\partial H^{\omega^{(\alpha)}}}{\partial a_1}(a) = \frac{\partial H^{\omega^{(\alpha)}}}{\partial a_2}(a) = \frac{\partial H^{\omega^{(\alpha)}}}{\partial a_3}(a) = 0,$$

we obtain $\omega^{(\alpha)} = 0$ and $\mathscr{A}_\alpha$ is transparent for $\alpha \geqslant 4$ (see also [5,8]).

Case 3: $4/\alpha \notin \mathbb{N}$ $(0 < \alpha < 4)$. Then $\mathscr{A}_\alpha = \mathscr{L}_\mu$ and we have (see Fig. 7)

$$n_\alpha = 3 + \mu + \tfrac{1}{2}\mu(\mu+1) \text{ with } \mu = \lfloor 4/\alpha \rfloor.$$

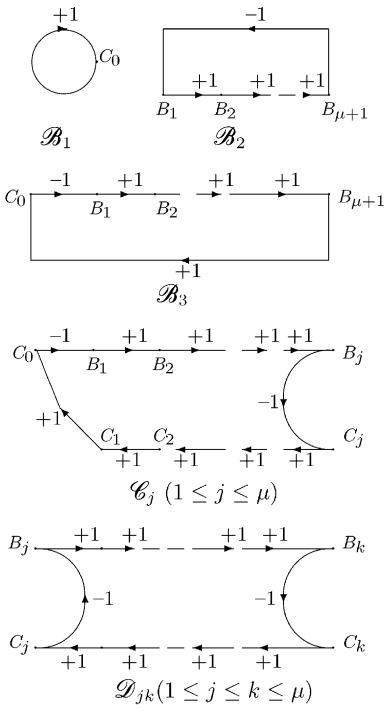


Fig. 7. Simple circuits of $\mathscr{L}_\mu$.

For any $a = (a_l)_{1 \leqslant l \leqslant n_\alpha} \in \mathbb{R}_+^{n_\alpha} \setminus \{O\}$ and any $j,k \in \mathbb{N}$ $(1 \leqslant j \leqslant k \leqslant \mu)$, we define

$$b_1 := a_1, \quad b_2 := a_2, \quad b_3 := a_3, \quad c_j := a_{j+3} \quad \text{and} \quad d_{jk} := a_{j\mu-(1/2)(j-1)j+k+3}.$$

i.e., renumber the coordinates of a by following the indices of simple circuits. So

1. $\lambda_{C_0,+1}(a) = b_1 + b_3 + \sum_{j=1}^{\mu} c_j$,
   $\lambda_{C_0,-1}(a) = 0$,
2. $\lambda_{B_1,+1}(a) = 0$,
   $\lambda_{B_1,-1}(a) = b_2 + b_3 + \sum_{j=1}^{\mu} c_j + \sum_{k=1}^{\mu} d_{1k}$,
3. $\lambda_{B_j,+1}(a) = b_2 + b_3 + \sum_{k=j}^{\mu} c_k + \sum_{k=1}^{j-1} \sum_{l=j}^{\mu} d_{kl}$,
   $\lambda_{B_j,-1}(a) = \sum_{k=j}^{\mu} d_{jk}$ $(2 \leqslant j \leqslant \mu)$,
4. $\lambda_{B_{\mu+1},+1}(a) = b_2 + b_3$,
   $\lambda_{B_{\mu+1},-1}(a) = 0$,
5. $\lambda_{C_j,+1}(a) = \sum_{k=j+1}^{\mu} c_k + \sum_{k=1}^{j} \sum_{l=j+1}^{\mu} d_{kl}$,
   $\lambda_{C_j,-1}(a) = c_j + \sum_{k=1}^{j} d_{kj}$ $(1 \leqslant j \leqslant \mu - 1)$,
6. $\lambda_{C_\mu,+1}(a) = 0$,
   $\lambda_{C_\mu,-1}(a) = c_\mu + \sum_{l=1}^{\mu} d_{l\mu}$.

Then, for any positive number ω and any point $a \in \mathbb{R}_+^{n_\alpha} \setminus \{O\}$, we have

$$\lambda(a) = b_1 + (\mu+1)b_2 + (\mu+2)b_3 + \sum_{j=1}^{\mu}(2j+1)c_j + \sum_{k=1}^{\mu}\sum_{l=k}^{\mu} 2(l-k+1)d_{kl},$$

$$H^\omega(a) = \lambda(a)\omega^2 - \sum_{j=2}^{\mu} \frac{4\lambda_{B_j,+1}(a)\lambda_{B_j,-1}(a)}{\lambda_{B_j}(a)} - \sum_{k=1}^{\mu-1} \frac{4\lambda_{C_k,+1}(a)\lambda_{C_k,-1}(a)}{\lambda_{C_k}(a)}.$$

To simplify the notations, for any integer j $(1 \leqslant j \leqslant \mu)$, define

$$\beta_j^{(\pm)} = \lambda_{B_j,\pm 1}(a), \quad \beta_j = \lambda_{B_j}(a) \quad \text{and} \quad \gamma_j^{(\pm)} = \lambda_{C_j,\pm 1}(a), \quad \gamma_j = \lambda_{C_j}(a).$$

Taking the weak partial derivatives of H^ω with respect to its variables, we obtain

7. $\frac{\partial H^\omega}{\partial b_1}(a) = \omega^2$,
8. $\frac{\partial H^\omega}{\partial b_2}(a) = (\mu+1)\omega^2 - 4\sum_{j=2}^{\mu}\left(\frac{\beta_j^{(-)}}{\beta_j}\right)^2$,
9. $\frac{\partial H^\omega}{\partial b_3}(a) = (\mu+2)\omega^2 - 4\sum_{j=2}^{\mu}\left(\frac{\beta_j^{(-)}}{\beta_j}\right)^2$,
10. $\frac{\partial H^\omega}{\partial c_1}(a) = 3\omega^2 - 4\left(\frac{\gamma_1^{(+)}}{\gamma_1}\right)^2$,
11. $\frac{\partial H^\omega}{\partial c_j}(a) = (2j+1)\omega^2 - 4\sum_{k=2}^{j}\left(\frac{\beta_k^{(-)}}{\beta_k}\right)^2 - 4\sum_{k=1}^{j-1}\left(\frac{\gamma_k^{(-)}}{\gamma_k}\right)^2 - 4\left(\frac{\gamma_j^{(+)}}{\gamma_j}\right)^2 \quad (2 \leqslant j \leqslant \mu)$,
12. $\frac{\partial H^\omega}{\partial d_{11}}(a) = 2\omega^2 - 4\left(\frac{\gamma_1^{(+)}}{\gamma_1}\right)^2$,
13. $\frac{\partial H^\omega}{\partial d_{1j}}(a) = 2j\omega^2 - 4\sum_{k=2}^{j}\left(\frac{\beta_k^{(-)}}{\beta_k}\right)^2 - 4\sum_{k=1}^{j-1}\left(\frac{\gamma_k^{(-)}}{\gamma_k}\right)^2 - 4\left(\frac{\gamma_j^{(+)}}{\gamma_j}\right)^2 \quad (2 \leqslant j \leqslant \mu)$,
14. $\frac{\partial H^\omega}{\partial d_{jj}}(a) = 2\omega^2 - 4\left(\frac{\beta_j^{(+)}}{\beta_j}\right)^2 - 4\left(\frac{\gamma_j^{(+)}}{\gamma_j}\right)^2 \quad (2 \leqslant j \leqslant \mu - 1)$,
15. $\frac{\partial H^\omega}{\partial d_{jk}}(a) = 2(k-j+1)\omega^2 - 4\sum_{l=j+1}^{k}\left(\frac{\beta_l^{(-)}}{\beta_l}\right)^2 - 4\left(\frac{\beta_j^{(+)}}{\beta_j}\right)^2 - 4\sum_{l=j}^{k-1}\left(\frac{\gamma_l^{(-)}}{\gamma_l}\right)^2 - 4\left(\frac{\gamma_k^{(+)}}{\gamma_k}\right)^2$
$(2 \leqslant j < k \leqslant \mu)$,
16. $\frac{\partial H^\omega}{\partial d_{\mu\mu}}(a) = 2\omega^2 - 4\left(\frac{\beta_\mu^{(+)}}{\beta_\mu}\right)^2$.

In particular, for $\mu = 1$, we have $n_\alpha = 5$ and the simple circuits are numbered as $\mathscr{B}_1$, $\mathscr{B}_2$, $\mathscr{B}_3$, $\mathscr{C}_1$ and $\mathscr{D}_{11}$. Hence for any $a \in \mathbb{R}_+^5 \setminus \{O\}$, we obtain

$$\frac{\partial H^\omega}{\partial b_1}(a) = \omega^2, \quad \frac{\partial H^\omega}{\partial b_2}(a) = 2\omega^2, \quad \frac{\partial H^\omega}{\partial b_3}(a) = 3\omega^2,$$

$$\frac{\partial H^\omega}{\partial c_1}(a) = 3\omega^2, \quad \frac{\partial H^\omega}{\partial d_{11}}(a) = 2\omega^2.$$

Then by Theorem 2, we have $\omega^{(\alpha)}=0$ and $\mathscr{A}_\alpha$ is transparent too.

Suppose $\mu \geqslant 2$. Remark that for the circuit $\mathscr{C}=\mathscr{D}_{1\mu}\mathscr{D}_{11}\cdots\mathscr{D}_{\mu\mu}$, we have

$$\lambda(a(\mathscr{C}))=4\mu \quad \text{and} \quad v(a(\mathscr{C}))=4(\mu-1).$$

Then from Equality (10) and the fact $\mu \geqslant 2$, we obtain

$$\omega := \omega^{(\alpha)} \geqslant \sqrt{\frac{v(a(\mathscr{C}))}{\lambda(a(\mathscr{C}))}} = \sqrt{\frac{\mu-1}{\mu}} > 0.$$

Let $a \in \mathbb{R}_+^{n_\alpha} \setminus \{O\}$ be a point satisfying Theorem 2. For any $j \in \mathbb{N}$ $(1 \leqslant j \leqslant n_\alpha)$, we have $\partial H^\omega/\partial a_j(a) \geqslant 0$. Hence from Relations (7)–(9), we deduce

$$\frac{\partial H^\omega}{\partial b_1}(a)=\omega^2>0 \quad \text{and} \quad \frac{\partial H^\omega}{\partial b_3}(a)=\omega^2+\frac{\partial H^\omega}{\partial b_2}(a)\geqslant \omega^2>0.$$

Similarly for any integer j $(1 \leqslant j \leqslant \mu)$, by Relations (10)–(13), we obtain

$$\frac{\partial H^\omega}{\partial c_j}(a)=\omega^2+\frac{\partial H^\omega}{\partial d_{1j}}(a)>0.$$

Thus by Theorem 2, we have necessarily $b_1=b_3=c_j=0$ $(1 \leqslant j \leqslant \mu)$.

Now for any integers j, k $(1 \leqslant j \leqslant k \leqslant \mu)$, put

$$(E_{jk}) \quad \frac{\partial H^\omega}{\partial d_{jk}}(a)=0.$$

From Equations (E_{jj}) $(1 \leqslant j \leqslant \mu)$ and the fact $\beta_1^{(+)}=0$ and $\gamma_\mu^{(+)}=0$, we obtain

$$\left(\frac{\beta_j^{(+)}}{\beta_j}\right)^2+\left(\frac{\gamma_j^{(+)}}{\gamma_j}\right)^2=\frac{1}{2}\,\omega^2. \tag{24}$$

Similarly from Relations (E_{1j}) with $2 \leqslant j \leqslant \mu$, we obtain

$$\sum_{k=2}^{j}\left(\frac{\beta_k^{(-)}}{\beta_k}\right)^2+\sum_{k=1}^{j-1}\left(\frac{\gamma_k^{(-)}}{\gamma_k}\right)^2+\left(\frac{\gamma_k^{(+)}}{\gamma_k}\right)^2=\frac{1}{2}\,j\omega^2$$

which is equivalent to

$$\left(\frac{\beta_2^{(-)}}{\beta_2}\right)^2+\left(\frac{\gamma_1^{(-)}}{\gamma_1}\right)^2+\left(\frac{\gamma_2^{(+)}}{\gamma_2}\right)^2=\omega^2,$$

$$\left(\frac{\beta_j^{(-)}}{\beta_j}\right)^2+\left(\frac{\gamma_{j-1}^{(-)}}{\gamma_{j-1}}\right)^2+\left(\frac{\gamma_j^{(+)}}{\gamma_j}\right)^2=\frac{1}{2}\,\omega^2+\left(\frac{\gamma_{j-1}^{(+)}}{\gamma_{j-1}}\right)^2 \ (3 \leqslant j \leqslant \mu).$$

Then by Relations (24) and the fact $\beta_1^{(+)}=0$ and $\gamma_\mu^{(+)}=0$, we obtain,

$$\left(\frac{\beta_j^{(-)}}{\beta_j}\right)^2+\left(\frac{\gamma_{j-1}^{(-)}}{\gamma_{j-1}}\right)^2=\left(\frac{\beta_j^{(+)}}{\beta_j}\right)^2+\left(\frac{\gamma_{j-1}^{(+)}}{\gamma_{j-1}}\right)^2 \ (2 \leqslant j \leqslant \mu),$$

which implies, by noting that $\beta_j^{(-)}+\beta_j^{(+)}=\beta_j$ and $\gamma_j^{(-)}+\gamma_j^{(+)}=\gamma_j$, the equality

$$\frac{\beta_j^{(-)}}{\beta_j}=\frac{\gamma_{j-1}^{(+)}}{\gamma_{j-1}} \quad \text{and} \quad \frac{\beta_j^{(+)}}{\beta_j}=\frac{\gamma_{j-1}^{(-)}}{\gamma_{j-1}}. \tag{25}$$

For any integer j $(1\leqslant j\leqslant \mu)$, define $x_j=\beta_j^{(+)}/\beta_j$. From Relations (24), (25) and the fact $\beta_1^{(+)}=0$, we deduce

$$\begin{cases} x_1=0, \\ x_j^2+(1-x_{j+1})^2=\frac{1}{2}\omega^2 \quad (1\leqslant j\leqslant \mu), \\ x_{\mu+1}=1. \end{cases} \tag{26}$$

We can easily verify that the system of equations (E_{jk}) $(1\leqslant j\leqslant k\leqslant \mu)$ is equivalent to that of equations (25) and (26).

For any $j\in\mathbb{N}$ $(1\leqslant j\leqslant \mu+1)$, put $y_j=1-x_{\mu+2-j}$. By Relations (26), we have

$$\begin{cases} y_1=0, \\ (1-y_{j+1})^2+y_j^2=\frac{1}{2}\,\omega^2 \quad (1\leqslant j\leqslant \mu), \\ y_{\mu+1}=1. \end{cases}$$

Hence for any integer j $(1\leqslant j\leqslant \mu+1)$, we must have $x_j=y_j=1-x_{\mu+2-j}$. Then

$$\begin{aligned} \frac{\partial H^{\omega}}{\partial b_2}(a) &= (\mu+1)\omega^2-4\sum_{j=2}^{\mu}\left(\frac{\beta_j^{(-)}}{\beta_j}\right)^2 \\ &= (\mu+1)\omega^2-4\sum_{j=2}^{\mu}(1-x_j)^2 \\ &= (\mu+1)\omega^2-2\sum_{j=2}^{\mu}(1-x_j)^2-2\sum_{j=2}^{\mu}(1-x_{\mu+2-j})^2 \\ &= (\mu+1)\omega^2-2\sum_{j=1}^{\mu}((1-x_{j+1})^2+x_j^2) \\ &= (\mu+1)\omega^2-2\sum_{j=1}^{\mu}\frac{1}{2}\,\omega^2 \\ &= \omega^2>0. \end{aligned}$$

So by Theorem 2, we have $b_2=0$. Note that if we have known x_j $(1\leqslant j\leqslant \mu)$ which may be calculated by Relations (26), we can determine d_{ij} $(1\leqslant j\leqslant k\leqslant \mu)$ by Relations (25). In other words, if the system of equations (26) has a solution, then by Theorem 2, the positive number ω decided by (26) is the opacity $\omega^{(\alpha)}$. Below we shall show that for any integer μ $(\mu\geqslant 2)$, the system of equations (26) has indeed a solution ϖ_μ (by Theorem 2, such a solution is unique) and we determine in the meantime the corresponding point a^{ϖ_μ}.

For any number ω $(0 \leqslant \omega \leqslant 1)$ and any $x \in [0, \omega^2/2]$, define

$$f_\omega(x) = 1 - \sqrt{\tfrac{1}{2}\omega^2 - x^2}.$$

Put $\mathbb{D}_1 = [0,1]$ and $\varpi_2 = 1/\sqrt{2}$. For any $\omega \in \mathbb{D}_1$, define

$$g_1(\omega) := f_\omega(0) = 1 - \frac{\sqrt{2}}{2}\,\omega.$$

Then set $y_1 = g_1(1) = 1 - (\sqrt{2}/2)$. Clearly the quadruplet $(\mathbb{D}_1, \varpi_2, g_1, y_1)$ satisfies
$(a)_1$ $\varpi_2 < 1$, $[\varpi_2, 1] \subset \mathbb{D}_1$ and $y_1 = g_1(1) < 1/2$,
$(b)_1$ the positive function g_1 is continuous and strictly decreasing on $\mathbb{D}_1$,
$(c)_1$ $g_1(\varpi_2) = \varpi_2/\sqrt{2}$.

Below by induction on the natural number μ $(\mu \geqslant 1)$, we shall construct a quadruplet $(\mathbb{D}_\mu, \varpi_{\mu+1}, g_\mu, y_\mu)$ which verifies
$(a)_\mu$ $\varpi_{\mu+1} < 1$, $[\varpi_{\mu+1}, 1] \subset \mathbb{D}_\mu$ and $y_\mu := g_\mu(1) < \frac{1}{2}$,
$(b)_\mu$ the positive function g_μ is continuous and strictly decreasing on $\mathbb{D}_\mu$,
$(c)_\mu$ $g_\mu(\varpi_{\mu+1}) = \varpi_{\mu+1}/\sqrt{2}$.

The case $\mu = 1$ has already been treated above. Suppose that we have already defined the quadruplet $(\mathbb{D}_{\mu-1}, \varpi_\mu, g_{\mu-1}, y_{\mu-1})$ with $\mu \geqslant 2$ and it satisfies the properties $(a)_{\mu-1}$, $(b)_{\mu-1}$ and $(c)_{\mu-1}$. For any $\omega \in \mathbb{D}_{\mu-1}$, define

$$h_{\mu-1}(\omega) := g_{\mu-1}(\omega) - \frac{1}{\sqrt{2}}\,\omega.$$

The function $h_{\mu-1}$ is continuous and strictly decreasing on $\mathbb{D}_{\mu-1}$. Define

$$\mathbb{D}_\mu = \{\omega \in \mathbb{D}_{\mu-1} \mid h_{\mu-1}(\omega) \leqslant 0\}.$$

Clearly $\varpi_\mu \in \mathbb{D}_\mu$. Hence $[\varpi_\mu, 1] \subset \mathbb{D}_\mu$ as $h_{\mu-1}$ is strictly decreasing on $\mathbb{D}_{\mu-1}$.

For any number $\omega \in \mathbb{D}_\mu$, define

$$g_\mu(\omega) := f_\omega(g_{\mu-1}(\omega)) \quad \text{and} \quad h_\mu(\omega) := g_\mu(\omega) - \frac{1}{\sqrt{2}}\,\omega.$$

Then the functions g_μ and h_μ are continuous and strictly decreasing on $\mathbb{D}_\mu$.

For any $\omega \in \mathbb{D}_\mu$ and $\omega < 1$, we can easily prove the following inequality:

$$g_{\mu-1}(\omega) < g_\mu(\omega). \tag{27}$$

In particular, $g_\mu(\varpi_\mu) > g_{\mu-1}(\varpi_\mu)$ and thus, $h_\mu(\varpi_\mu) > 0$. Since $y_{\mu-1} < \frac{1}{2}$, then we obtain $y_\mu = f_1(y_{\mu-1}) < \frac{1}{2}$. Hence $h_\mu(1) < 0$ as $1/2 < 1/\sqrt{2}$. Now by the famous Mean Value Theorem, we can find $\varpi_{\mu+1} \in [\varpi_\mu, 1]$ such that $h_\mu(\varpi_{\mu+1}) = 0$. So $[\varpi_{\mu+1}, 1] \subset \mathbb{D}_\mu$ and $(\mathbb{D}_\mu, \varpi_{\mu+1}, g_\mu, y_\mu)$ verifies the properties $(a)_\mu$, $(b)_\mu$ and $(c)_\mu$.

Fix $\mu \in \mathbb{N}$ $(\mu \geqslant 2)$. For any integer j $(1 \leqslant j \leqslant \mu + 1)$, we define $x_j = g_{j-1}(\varpi_\mu)$ with $g_0 \equiv 0$. Evidently for any integer j $(1 \leqslant j \leqslant \mu+1)$, the number x_j is well-defined since we have $\varpi_\mu \in \mathbb{D}_{j-1}$ with $\mathbb{D}_0 = [0,\ 1]$. Moreover these numbers x_j's and ϖ_μ satisfy the system of equations (26).

Now we define a point a^{ϖ_μ} such that the couple $(\varpi_\mu, a^{\varpi_\mu})$ verifies Theorem 2.

Remark that for any integer j $(1 \leqslant j \leqslant \mu)$, we have $\varpi_\mu \in \mathbb{D}_j$ and $\varpi_\mu < 1$. Thus by Relations (27), we have $g_{j-1}(\varpi_\mu) < g_j(\varpi_\mu)$, i.e., $x_j < x_{j+1}$. In particular, for any integer j $(2 \leqslant j \leqslant \mu)$, we have $0 < x_j < 1$.

For any integer j $(2 \leqslant j \leqslant \mu-1)$, we define by recurrence $z_j=(1-x_{j+1})z_{j-1}/x_j$ with $z_1=1$. Then put $d_{11} := x_2 z_1/(1-x_2)$, $d_{(j-1)j} := z_{j-1}$, $d_{jj} := (x_{j+1}-x_j)/x_j z_{j-1}$ $(2 \leqslant j \leqslant \mu)$ and $d_{kl} := 0$ $(1 \leqslant k \leqslant l-2 \leqslant \mu-2)$. Finally we define $a^{\varpi_\mu} = (a_j)_{1 \leqslant j \leqslant n_\alpha} \in \mathbb{R}_+^{n_\alpha} \setminus \{O\}$ as follows:

$$a_j := 0 \ (1 \leqslant j \leqslant \mu+3) \quad \text{and} \quad a_{k\mu-(1/2)(k-1)k+l+3} \ (1 \leqslant k \leqslant l \leqslant \mu).$$

We can verify without difficulty that the couple $(\varpi_\mu, a^{\varpi_\mu})$ satisfies the conditions of our Theorem 2. Thus $\varpi_\mu = \omega^{(\alpha)}$ with $\mu = \lfloor 4/\alpha \rfloor$.

Case 4: $4/\alpha \in \mathbb{N}$ $(0 < \alpha < 4)$. Put $\mu = 4/\alpha$. Then we have $\mathscr{A}_\alpha = \mathscr{N}_\mu$ and we leave for the reader as a good exercise to verify, just in the same manner as above, the equality $\omega(\mathscr{N}_\mu) = \omega(\mathscr{L}_\mu)$.

In conclusion we have shown the following result:

Theorem 7. *For any integer μ $(\mu \geqslant 1)$, the opacity $\varpi_\mu := \omega(\mathscr{L}_\mu) = \omega(\mathscr{N}_\mu)$ is uniquely determined by the equation $g_{\mu-1}(\varpi_\mu) = \varpi_\mu/\sqrt{2}$. Furthermore, the positive sequence $(\varpi_\mu)_{\mu \geqslant 1}$ is strictly increasing and converges to 1 as $\varpi_\mu \geqslant \sqrt{(\mu-1)/\mu}$.*

Remark 1. By Relations (26), we have

$$\sum_{j=2}^{\mu} (2x_j - 1)^2 = \mu(\varpi_\mu^2 - 1) + 1 \quad \text{with } \mu \geqslant 2.$$

Then we obtain $\varpi_\mu^2 \geqslant 1 - 1/\mu$ which also implies

$$\lim_{\mu \to \infty} \varpi_\mu = 1.$$

Remark 2. Put $\varpi_0 = 0$ and $\varpi_\infty = 1$. For any nonnegative number α, we have

$$\varpi_{\lfloor 4/\alpha \rfloor} = \omega^{(\alpha)} = \omega(\mathscr{A}_\alpha)$$

where by convention, we define $\lfloor 4/0 \rfloor = \infty$. As a result, we obtain

$$\lim_{\alpha \to 0} \omega^{(\alpha)} = \omega^{(0)}$$

which means that the function $\alpha \to \omega^{(\alpha)}$ is continuous at $\alpha=0$. Better it was shown that in a certain sense the mapping $\alpha \to (\mathscr{A}_\alpha, \psi_\alpha)$ is continuous on $[0, +\infty)$ and uniformly continuous on $[\alpha_0, +\infty)$ for any $\alpha_0 > 0$ (see [3,7]). This result is quite surprising for $\mathscr{A}_\alpha$ $(\alpha > 0)$ contains at least $\lfloor 4/\alpha \rfloor + 1$ states. Moreover, it also reflects the continuity of our discrete physical models!

Some numerical results:

$$\varpi_0 = 0, \quad \varpi_1 = 0, \quad \varpi_2 = \frac{\sqrt{2}}{2}, \quad \varpi_3 = 2(\sqrt{2}-1), \quad \varpi_4 = \frac{5}{8}\sqrt{2}, \ \ldots, \ \varpi_\infty = 1.$$

In fact, with the help of the software Maple, it is quite easy to solve the equation

$$g_{\mu-1}(\varpi_\mu) = \varpi_\mu/\sqrt{2} \ (\mu \geqslant 1).$$

Remark also here $\varpi_3^2 = 4(3-2\sqrt{2}) \notin \mathbb{Q}$ although $\Sigma = \{1, -1\} \subset \mathbb{Q}$. This concrete example confirms our remark about Corollary 2.

10. Further study

Until now we have only considered complete deterministic automata. It is possible to generalize all the preceding results to the most general automata. Often we need make some technical efforts. But sometimes certain results may be simplified and presented in a more appropriate form.

Acknowledgements

We thank Michel Mendès France for his help and his remarks. We appreciate Pierre Liardet and Nathalie Loraud for some interesting discussions. We also thank our anonymous referees for their efficient work. Finally, we thank National Natural Science Foundation of China and Morningside Center of Mathematics (CAS) for their financial support.

References

[1] G.-L. Chen, J.-Y. Yao, Characterization of opaque automata, Discrete Math. 247, (2002) 65–78.
[2] S. Eilenberg, Automata, Languages and Machines, Vol. A, Academic Press, New York, 1974.
[3] T. Kamae, M. Mendès France, A continuous family of automata: the Ising automata, Ann. Inst. H. Poincaré, Phys. Théor. 64 (1996) 349–372.
[4] N. Loraud, Numérations généralisées, langages et automates, Thèse, Université de Provence, 1996.
[5] M. Mendès France, Opacity of an automaton. Application to the inhomogeneous Ising chain, Comm. Math. Phys. 139 (1991) 341–352.
[6] M. Schwartz, Information Transmission, Modulation, and Noises, McGraw-Hill, New York, 1970.
[7] J.-Y. Yao, Contribution à l'étude des automates finis, Thèse, Université Bordeaux I, 1996.
[8] J.-Y. Yao, Opacités des automates finis, Discrete Math. 202 (1999) 279–298.